

HUAWEI CLOUD Compliance with Indonesia Privacy Protection Regulations

Issue	2.2
Date	2024-07-17



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei 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 Cloud Services Privacy Protection Responsibilities Sharing Model	3
3 Overview of Indonesia Privacy Regulations	5
3.1 Background of Indonesia Privacy Regulations	5
3.2 Roles and Basic Obligations	5
3.3 HUAWEI CLOUD's Role under Indonesia Privacy Regulations	8
4 How HUAWEI CLOUD Responses to the Indonesia Privacy Compliance Requirements	9
4.1 HUAWEI CLOUD Privacy Commitment	9
4.2 HUAWEI CLOUD Basic Privacy Protection Principles	9
4.3 HUAWEI CLOUD's Compliance Measures in Response to Indonesia Privacy Regulations	10
5 How HUAWEI CLOUD Supports Customers to Comply with Indonesia Privacy Regulations	24
5.1 Customers' Privacy Protection Responsibilities	24
5.2 How HUAWEI CLOUD Products and Services Help Customers Implement Content Data Privacy and Security	34
6 HUAWEI CLOUD Privacy Protection Related Certifications	39
7 Conclusion	44
8 Version History	45

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 Indonesia.

1.2 Purpose of Publication

This document is intended to help customers understand:

1. HUAWEI CLOUD's privacy protection responsibility model;
2. Indonesia privacy related legal requirements;
3. HUAWEI CLOUD's responsibilities on compliance with Indonesia privacy regulations, as specified in the responsibility model;
4. HUAWEI CLOUD's controls and achievements in privacy management;
5. Customers' responsibilities and obligations when falling under the jurisdiction of Indonesia privacy regulations, as specified in the responsibility model;
6. How to leverage HUAWEI CLOUD's security products and services to achieve privacy compliance.

1.3 Basic Definitions

- **Personal Data**
Personal data is data about an identified or identifiable individual individually or in combination with other information either directly or indirectly through electronic or non-electronic systems.
- **Personal Data Subject**
Personal data subject is a natural person to whom personal data is attached.
- **Personal Data Controller**
Personal data controller means any person, public body and international organization acting individually or jointly in determining the purposes and exercising control over the processing of personal data.
- **Personal Data Processor**

Personal data processor means any person, public body and international organization acting singly or jointly in performing personal data processing on behalf of the personal data controller.

- **Electronic System User**

User shall be every person, state administrator, business entity, and community utilizing goods, services, facilities, or information provided by electronic system operators.

- **Electronic System Operator**

Any person, state administrator, business entity, and community who provides, manages and/or operates electronic systems, either individually or collectively to electronic system users for their own needs and/or the needs of other parties.

Electronic system operators for public purposes: Any electronic system operation authorized by a state agency or an institution designated by a state agency based on public purposes.

Electronic system operators for private purposes: Electronic system operations authorized by a private person or business entity based on private purposes.

- **HUAWEI CLOUD**

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

- **Customer**

Registered user who has 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.

- **Content Data**

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

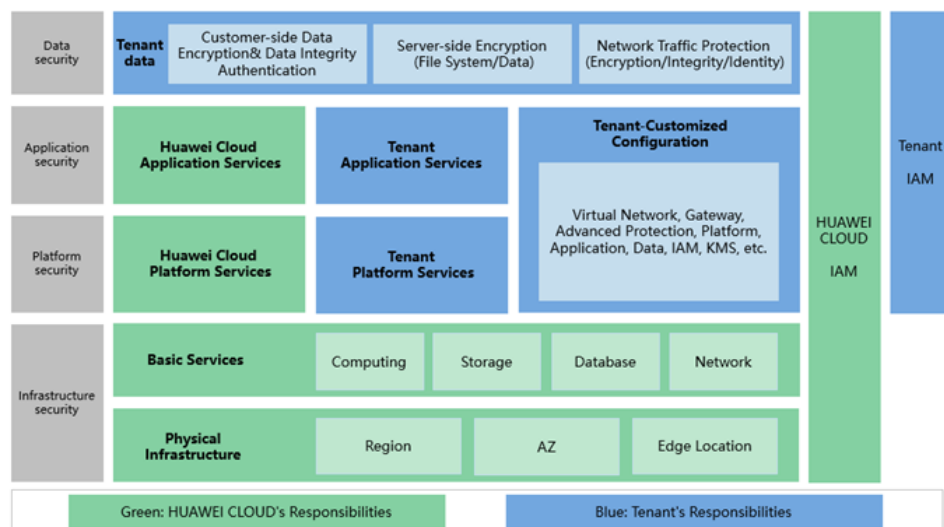
- **Personal Data Processing**

Operations on personal data, including obtainment and collection, processing and analysis, storage, reparation and renewal, announcement, transfer, dissemination, disclosure, deletion, and etc.

2 Cloud Services Privacy Protection Responsibilities Sharing Model

Due to the complexity of cloud service business model, the privacy protection is not the sole responsibility of one single party, but requires the joint efforts of both the 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 various 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 model, 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 of personal data collected or processed during business operations and compliance, but also responsible for the **platform security**, which means providing secure and compliant infrastructure, cloud platform and software applications related to cloud services to tenants.

- **Protection of Tenant's Privacy:** HUAWEI CLOUD identifies and protects tenants' personal data. HUAWEI CLOUD formulates privacy protection policies from company policies, processes and operation levels and adopts active privacy control measures, such

as anonymization, data encryption, system and platform security protection, and comprehensively protect the security of tenants.

- **Platform and Tenant Security Support:** HUAWEI CLOUD is responsible for the security and compliance of the platform and infrastructure involved in the cloud service, ensuring the applications' security and platform security levels to comply with the requirements of applicable privacy protection laws and regulations. At the same time, HUAWEI CLOUD provides tenants with a variety of privacy protection technologies and services, such as access control, identity authentication, data encryption, logging and auditing functions, in order to help tenants protect their privacy according to their commercial requirements.

Tenant: As the purchaser of HUAWEI CLOUD's products and services, tenants are free to decide on how to use the products or services and how to use cloud products or services to store and process content data, which may include personal data. Therefore, 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 the security and privacy of personal data, and finally select appropriate privacy protection measures. Specific measures include security configuration based on business and privacy protection requirements, such as operating system configuration, network settings, security protection, database encryption policy, and set appropriate access controls and password policies.
- **Respond to Personal Data Subject's Rights:** Customers shall guarantee the rights of personal data subjects and respond to their requests in a timely manner. In the case of a personal data breach, the customer shall take adequate actions in accordance with regulatory requirements, such as notifying both the regulators and the personal data subjects or take mitigation measures.

3

Overview of Indonesia Privacy Regulations

3.1 Background of Indonesia Privacy Regulations

- **Law No. 27 of 2022 concerning Personal Data Protection (PDP Law):** This law was submitted to the Indonesian Parliament in 2020, which promulgated the law on October 17, 2022. The provisions of this law are based on the GDPR and introduce some concepts stipulated in the GDPR. (e.g., concepts of data controllers and data processors, classification of general and specific personal data). As a special regulation for the protection of personal data in Indonesia, the PDP Law has changed the fragmented situation of the country's previous personal data protection regulations and made them more systematic. According to the PDP Law, after the law takes effect, all laws and regulations related to personal data protection in Indonesia shall remain valid without violating the provisions of the PDP Law.
- **Government Regulation No.71 of 2019 (GR71/2019):** This regulation was issued in October 2019, and amended Government Regulation No.82 of 2012 Concerning Electronic System and Transaction Operation. It sets requirements on electronic system operation, electronic agencies, electronic transaction operation, electronic certification operation, reliability certification institutions, domain management, and etc.
- **Minister of Communications & Informatics Regulation No.20 of 2016 regarding the Protection of Personal Data in an Electronic System (MOCI 20/2016):** This regulation was issued in December 2016. As the implementation method of personal data protection requirements in EIT, it sets requirements on the obtainment and collection, processing and analysis, storage, disclosure of personal data, personal data subjects' rights, electronic system operators' obligations, and etc.
- **Law No. 11 of 2008 regarding Electronic Information and Transactions (EIT):** This law was issued in 2008, and was amended in 2016. It sets requirements on electronic information, records, signatures, the provision of electronic system and electronic certification, electronic transactions, domain, intellectual property, privacy protection rights, and etc.

3.2 Roles and Basic Obligations

PDP Law defines the roles of personal data subject, personal data controller, and personal data processor.

Personal data subject shall be entitled to confidentiality of their personal data, filing complaints in the context of personal data dispute resolution with respect to failure in the protection of their personal data, updating or correcting, having access to and deleting their personal data, the right to withdraw the consent, and etc.

Personal data processor's basic obligations include processing personal data in accordance with the instructions of the personal data controller, maintaining the accuracy, completeness and consistency of personal data, documenting personal data processing activities, maintaining the security and confidentiality of personal data to prevent unauthorized processing and unauthorized access.

The basic obligations of the personal data controller are more extensive than those of the data processor, including:

1. **Personal Data Collection:** Collect personal data in a manner that is limited, specific, lawful, and fair. Prior to the personal data collection, notify personal data subjects and obtain their consent, unless other legal reasons are present.
2. **Personal Data Processing:** The processing of personal data is carried out in accordance with the objectives disclosed to the personal data subject. The processing of personal data is performed in an accurate, complete, non-misleading, up-to-date, accountable manner. Protect personal data from loss, misuse, unauthorized access, alteration, destruction or disclosure.
3. **Protection of Personal Data Subject's Rights:** The personal data subject's rights shall be protected during data processing. Personal data subjects shall be entitled to confidentiality of their personal data, filing complaints in the context of personal data dispute resolution with respect to failure in the protection of their personal data, updating or correcting, having access to and deleting their personal data, as well as the right to withdraw the consent.
4. **Data Retention:** Destroy personal data within the retention period or as required by regulations.
5. **Notice of Personal Data Breaches:** In the event of a personal data breach, notify the data subject and the supervisory authority in writing within 72 hours, and inform them of the personal data that has been breached, the time and manner of the personal data breach, and the remedial measures taken by the personal data controller in response to the personal data breach.
6. **Data Protection Impact Assessment:** A data protection impact assessment shall be carried out if the processing operation may pose a high risk to the rights and freedoms of the personal data subject due to its nature, scope, context and purpose.
7. **Data Security:** Appropriate technical and organizational measures shall be taken to protect data security.
8. **Records of Processing Activities:** All personal data processing activities shall be recorded.
9. **DPO:** A DPO shall be appointed to fulfill personal data protection responsibilities.
10. **Cross-border Transfer of Data:** Personal data may be transferred to another country only if: ensure that the level of personal data protection in the country where the controller and/or the personal data processor receiving the transfer is located is not lower than the legal level; ensure that personal data is adequately protected if the foregoing conditions are not met; If the preceding two conditions are not met, the consent of the personal data subject shall be obtained.

EIT, MOCI 20/2016 and GR71/2019 define the roles of personal data subjects, electronic system users, and electronic system operators.

The personal data subject is the owner of personal data and shall be entitled to confidentiality of their personal data, filing complaints in the context of personal data dispute resolution with respect to failure in the protection of their personal data, updating or correcting, having access to and deleting their personal data, the right to withdraw the consent, and etc.

Electronic system users' basic obligations include maintaining the confidentiality of the personal data acquired, collected, processed and analyzed by them, using personal data only in accordance with their needs, protecting personal data along with documents containing personal data from the act of misuse, and being responsible for personal data in their control.

Electronic system operators' basic obligations cover the obligations of electronic system users, which include:

1. **Personal Data Collection:** Collect personal data in a manner that is limited, specific, lawful, and fair. Prior to the personal data collection, notify personal data subjects and obtain their consent, unless other legal reasons are present.
2. **Personal Data Processing:** The processing of personal data is carried out in accordance with the objectives disclosed to the personal data subject. The processing of personal data is performed in an accurate, complete, non-misleading, up-to-date, accountable manner. Protect personal data from loss, misuse, unauthorized access, alteration, destruction or disclosure.
3. **Protection of Personal Data Subject's Rights:** The personal data subjects' rights shall be protected during data processing. Personal data subjects shall be entitled to confidentiality of their personal data, filing complaints in the context of personal data dispute resolution with respect to failure in the protection of their personal data, updating or correcting, having access to and deleting their personal data, as well as the right to withdraw the consent.
4. **Data Retention:** Destroy personal data within the retention period or as required by regulations.
5. **Notice of Personal Data Breaches:** Electronic systems operators must provide written notice to personal data subjects when the providers fail to protect the data's confidentiality and must inform the personal data subjects of the potential damage from the breach. If the breach may cause the personal data subject harm, the electronic systems operator must confirm that the personal data subject received the breach notification. In the event of a serious breach, electronic systems operators must immediately secure the data and notify law enforcement and the Ministry of Communications and Information Technology (MOCI).
6. **Certification:** Obtain the necessary electronic system certification as required by laws and regulations.
7. **Processing Activity Records:** Provide audit track records on all activities of the electronic system managed by them.
8. **Providing a Contact Person:** A contact person, who is easily contacted by personal data subjects for the management of their personal data, should be provided.
9. **Data Localization:** Electronic system operators for public purposes should store and manage relevant electronic systems and electronic data in the territory of Indonesia, unless the domestically available technology is insufficient. Electronic system operators for private purposes may manage, process or store electronic system and electronic data outside the jurisdiction of Indonesia. The operator must allow the relevant authority and law enforcement agency to supervise it, including allowing the authority and law enforcement agency to access the electronic system and electronic data.

10. **Data Cross-border Transfer:** If electronic system operators need to transfer any personal data generated by government, regional governments, or individuals or entities residing in Indonesia outside of Indonesia, they must undergo a coordination process with MOCI.

3.3 HUAWEI CLOUD's Role under Indonesia Privacy Regulations

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 customers decide to use HUAWEI CLOUD services or applications to processing personal data included in content data, HUAWEI CLOUD is generally regarded as the personal data processor defined in PDP Law. HUAWEI CLOUD acts as the personal data controller defined in PDP Law when HUAWEI CLOUD collect personal data from customer for the customers' set up or management of their HUAWEI CLOUD account.

HUAWEI CLOUD acts as the personal 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 others 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 personal data subjects' requests, complying with Indonesia privacy protection laws and regulations requirements regarding limited disclosure, and finally taking actions to avoid data breaches.

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

In addition, based on the characteristics of HUAWEI CLOUD's business, HUAWEI CLOUD provides facilities or services based on customers' needs. For activities subject to EIT, MOCI 20/2016 and GR71/2019, in most cases, HUAWEI CLOUD is the electronic system operator, and the customer is the electronic system user. HUAWEI CLOUD undertakes the obligations of electronic system operators, while collects, processes, and stores personal data in compliance with legal requirements, and respond to personal data subjects' right requests.

When customers use HUAWEI CLOUD services to provide services subject to EIT, MOCI 20/2016 and GR71/2019 to other electronic system users, HUAWEI CLOUD will help customers fulfill the corresponding obligations.

4 How HUAWEI CLOUD Responses to the Indonesia Privacy Compliance Requirements

4.1 HUAWEI CLOUD Privacy Commitment

Cyber security and privacy protection are the cornerstones for the development of the digital and intelligent world. HUAWEI CLOUD has integrated cyber security and privacy protection into its cloud services promising to provide customers with stable, reliable, secure, trustworthy, and evolvable services while respecting and protecting customers' privacy.

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

4.2 HUAWEI CLOUD Basic Privacy Protection Principles

- **Lawfulness, Fairness and Transparency**
HUAWEI CLOUD processes personal data of personal data subjects lawfully, fairly and in a transparent manner.
- **Purpose Restriction**
HUAWEI CLOUD collects personal data for specific, explicit and lawful purposes and will not further process the data in a manner that is incompatible with those purposes.
- **Data Minimization**
When HUAWEI CLOUD processes personal data, personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed. Personal data will be anonymized or pseudonymized to the extent possible to reduce the risks for personal 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.
- **Minimize Storage Duration**

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

- **Integrity and Confidentiality**

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

- **Accountability**

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

4.3 HUAWEI CLOUD's Compliance Measures in Response to Indonesia Privacy Regulations

Based on the characteristics of HUAWEI CLOUD's business and the requirements of PDP Law, HUAWEI CLOUD, as a legal entity that processes personal data, assumes two roles of data controller and data processor in different scenarios.. HUAWEI CLOUD adopts the following privacy protection mechanisms and technologies to comply with the requirements of Indonesia privacy regulations.

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the data controller)	Measures Taken by HUAWEI CLOUD
Personal Data Collection	<ol style="list-style-type: none">1. Collect personal data in a manner that is limited, specific, lawful, and fair.2. Prior to the personal data collection, notify personal data subjects and obtain their consent, unless other legal reasons are present.	<ol style="list-style-type: none">1. HUAWEI CLOUD follows the basic principles of privacy protection of being lawful, fair, transparent, and data minimization. HUAWEI CLOUD will evaluate business needs before collecting personal data, collect only the minimum personal data required by the business, clarify the type of personal data collected, and select the appropriate and legal personal data collection basis.2. When a customer registers for an account, HUAWEI CLOUD clearly informs customers of the types of personal data to be collected, purposes, and legal basis of personal data collection and processing in the Privacy Policy Statement, so that customers can clearly understand related personal data processing activities and agree to them. When the scope or use purpose of personal data collected by the product or service changes,

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the data controller)	Measures Taken by HUAWEI CLOUD
		the privacy statement will be updated accordingly and customers will be asked again for their consent. Additional privacy notices 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.
Personal Data Processing	<ol style="list-style-type: none">1. The processing of personal data is carried out in accordance with the objectives disclosed to the personal data subject.2. The processing of personal data is performed in an accurate, complete, non-misleading, up-to-date, accountable manner. Protect personal data from loss, misuse, unauthorized access, alteration, destruction or disclosure.	<ol style="list-style-type: none">1. HUAWEI CLOUD clearly informs customers of the purposes of personal data processing in the Privacy Policy Statement and collects and processes personal data based on the purposes disclosed in the Privacy Policy Statement. HUAWEI CLOUD regularly conducts Privacy Impact Assessments for products and services that involve personal data in order to prevent the collection and processing of personal data in products and services beyond the scope required for their actual purposes.2. HUAWEI CLOUD attaches great importance to and takes appropriate physical, technical, and organizational measures to protect the security, accuracy, and integrity of personal data, including but not limited to:<ul style="list-style-type: none">● Sets up a privacy protection organization to identify and manage personal data protection risks.● Adopts strict data security and personal data protection policies, in accordance with the risk of the categories of data processed. Develops security breach response and data breach process to reduce privacy and security risks brought by personal data breaches and guide relevant departments to

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the data controller)	Measures Taken by HUAWEI CLOUD
		<p>handle personal data in compliance with laws and regulations.</p> <ul style="list-style-type: none">● Holds security and privacy protection training courses, tests, and publicity activities to raise employees' personal data protection awareness.● Takes reasonable and feasible measures to ensure that the personal data collected is minimal and relevant to what is necessary in relation to the purposes for which they are processed.● Takes a range of measures such as an entrance and exit control, entrance guard systems and CCTV system to ensure the physical security of the data centers to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.● Deploys access control mechanisms and implements hierarchical permission management on them based on service requirements and personnel levels to ensure that only authorized personnel can access personal data.● Clearly defines and assigns cyber security roles and responsibilities, and implements separation of duties (SOD) based on a risk assessment to reduce risks to prevent data processing systems from being used by unauthorized persons.● Encryption and pseudonymisation of personal data, as appropriate, using recommended industry standard protocols to prevent data breach and unauthorized access,● Degausses the discarded storage media before returning to the warehouse to ensure that software-based overwriting shall be

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the data controller)	Measures Taken by HUAWEI CLOUD
		<p>performed on media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction shall be performed.</p> <ul style="list-style-type: none">● Implements appropriate O&M security management and technical measures, including identity authentication and access control, change and event management, vulnerability management, configuration management, event logging, and continuously monitors cyber security events and threats, detects exceptions in a timely manner, and proactively takes measures to deal with them to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons.● Implements protection mechanisms such as DDoS protection to protect networks from attacks, develops vulnerability management policies, evaluation standards, and management processes to manage security vulnerabilities throughout the lifecycle. In addition, regularly runs vulnerability scanning programs to detect potential security vulnerabilities and promptly take countermeasures.● Strictly selects business partners and service providers and incorporates personal data protection requirements into commercial contracts, audits, and appraisal activities. <p>In addition, HUAWEI CLOUD has obtained multiple certifications in relation to privacy compliance international standard, including ISO 27701, ISO 29151, ISO 27018, BS 10012, the audit report of SOC2 Type 1 privacy principle, and etc. Customers can also understand personal data security controls within HUAWEI CLOUD's environment</p>

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the data controller)	Measures Taken by HUAWEI CLOUD
		through HUAWEI CLOUD security reports or certifications .
Protection of Personal Data Subject's Rights	The personal data subject's rights shall be protected during data processing. Personal data subjects shall be entitled to confidentiality of their personal data, filing complaints in the context of personal data dispute resolution with respect to failure in the protection of their personal data, updating or correcting, having access to and deleting their personal data, as well as the right to withdraw the consent.	In the Privacy Policy Statement , HUAWEI CLOUD clearly informs data subjects of their privacy rights, such as the right to access, correct, delete, object, restrict processing, portability, consent withdrawal, and complaints to regulators. HUAWEI CLOUD provides customers with convenient channels for exercising data subjects' rights. When a data subject submits a data subject's rights request to HUAWEI CLOUD, HUAWEI CLOUD will respond to the data subject's rights request in a timely manner.
Data Retention	Destroy personal data within the retention period or as required by regulations.	HUAWEI CLOUD clearly informs customers of the purposes of personal data processing in the Privacy Policy Statement . Unless otherwise required by laws or customers, HUAWEI CLOUD will retain personal data for a period of time that is necessary to achieve the processing purposes described in the Privacy Policy Statement . (The retention period of personal data may vary depending on the processing purpose and service). In addition, unless otherwise specified by applicable laws and regulations, HUAWEI CLOUD will anonymize or delete unnecessary personal data after the storage period expires after the customer deregisters the HUAWEI CLOUD account.
Notice of Personal Data Breaches	In the event of a personal data breach, notify the data subject and the supervisory authority in writing within 72 hours, and inform them of the personal data that has been breached, the time and manner of the personal data breach, and the remedial measures taken by the personal data controller in response to the personal data breach.	HUAWEI CLOUD has set up a 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

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the data controller)	Measures Taken by HUAWEI CLOUD
		<p>subjects' business, initiates the notification process according to the notification mechanism of security incidents, and notifies personal data subjects of the incident.</p> <p>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 regulatory filings will be conducted in accordance with local regulations.</p>
Data Protection Impact Assessment	A data protection impact assessment shall be carried out if the processing operation may pose a high risk to the rights and freedoms of the personal data subject due to its nature, scope, context and purpose.	<p>To effectively identify and control privacy risks, HUAWEI CLOUD conducts extensive privacy risk analysis and management in various cloud services.</p> <p>Service scenarios that pose high risks to the rights and freedoms of data subjects. HUAWEI CLOUD requires data protection impact assessment (DPIA) before processing personal data. The DPIA mainly includes identifying personal data items involved in business, business scenarios and processing, compliance analysis, possible impacts on data subjects, risk analysis, and risk control measures and plans. All privacy risk control requirements are incorporated into the design solution. Business can only be conducted if privacy risks are reduced to an acceptable level.</p>
Data Security	Appropriate technical and organizational measures shall be taken to protect data security.	HUAWEI CLOUD attaches great importance to and takes appropriate physical, technical, and organizational measures to protect the security, accuracy, and integrity of personal data. For details about the protection measures taken by HUAWEI CLOUD, see the Privacy Policy

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the data controller)	Measures Taken by HUAWEI CLOUD
		<p>Statement.</p> <p>In addition, HUAWEI CLOUD has obtained multiple certifications in relation to privacy compliance international standard, including ISO 27701, ISO 29151, ISO 27018, BS 10012, the audit report of SOC2 Type 1 privacy principle, and etc. Customers can also understand personal data security controls within HUAWEI CLOUD's environment through HUAWEI CLOUD security reports or certifications.</p>
Records of Processing Activities	All personal data processing activities shall be recorded.	<p>HUAWEI CLOUD retains activity records for privacy management activities:</p> <ul style="list-style-type: none">● A Privacy Impact Assessment will be performed before the service becomes available. The types of personal data, collection purpose of personal data and retention period of personal data will be listed in the assessment record.● During the service's daily operation and maintenance, in accordance with the requirements of the regulations, retain the information related to personal data subjects' right requests and responses, and the operation log of implementing security measures.
DPO	A DPO shall be appointed to fulfill personal data protection responsibilities.	Currently, HUAWEI CLOUD has set up a data protection officer. If you have any questions, comments, suggestions, etc., the customer can contact the Data Protection Officer at the email address provided in the Privacy Policy Statement .
Cross-border Transfer of Data	Personal data may be transferred to another country only if: ensure that the level of personal data protection in the country where the controller and/or the personal data processor receiving the transfer is located is not lower than the	HUAWEI CLOUD has stated in the Privacy Policy Statement that it will provide services to customers through HUAWEI CLOUD's global resources. Therefore, customers' personal data may be transferred to or accessed by HUAWEI CLOUD, HUAWEI CLOUD affiliates, and HUAWEI

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the data controller)	Measures Taken by HUAWEI CLOUD
	legal level; ensure that personal data is adequately protected if the foregoing conditions are not met; If the preceding two conditions are not met, the consent of the personal data subject shall be obtained.	<p>CLOUD partners in countries or regions where they are located. In this case, HUAWEI CLOUD will ensure that the transfer complies with relevant laws and regulations (including ensuring that overseas recipients comply with and fulfil relevant confidentiality and data protection obligations) and HUAWEI CLOUD Privacy Policy Statement.</p> <p>HUAWEI CLOUD has set up a privacy protection expert team to evaluate the level of personal data protection provided by the countries involved in data transmission and determine the legal basis for cross-border data transmission. For countries and regions where the business is located, HUAWEI CLOUD also has dedicated legal and privacy protection personnel to help HUAWEI CLOUD take necessary measures according to applicable privacy laws and regulations.</p>

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the data processor)	Measures Taken by HUAWEI CLOUD
Obligations of Personal Data Processors	<ol style="list-style-type: none">1. Processing personal data in accordance with the instructions of the personal data controller.2. Maintaining the accuracy, completeness and consistency of personal data.3. Maintaining the security and confidentiality of personal data to prevent unauthorized processing and unauthorized access.4. Documenting personal data processing	<p>HUAWEI CLOUD only processes data according to the customer's instructions. The customer shall collect personal data in a fair and transparent manner and ensure that the purpose is appropriate. The customer shall not use personal data for purposes other than those agreed upon. In addition, the basis, purpose, scope, accuracy, and data retention period of content data collection are managed by the customer.</p> <p>As a personal data processor, HUAWEI CLOUD takes appropriate physical, technical, and organizational measures to help customers protect the security, accuracy, and integrity of personal</p>

	activities.	<p>data to meet security obligations specified by laws. For details about the protection measures taken by HUAWEI CLOUD as a personal data processor, see the Data Processing Addendum.</p> <p>HUAWEI CLOUD retains activity records for privacy management activities:</p> <ul style="list-style-type: none">● A Privacy Impact Assessment will be performed before the service becomes available. The types of personal data, collection purpose of personal data and retention period of personal data will be listed in the assessment record.● During the service's daily operation and maintenance, in accordance with the requirements of the regulations, retain the information related to personal data subjects' right requests and responses, and the operation log of implementing security measures.
--	-------------	---

Based on the characteristics of HUAWEI CLOUD's business and the requirements of EIT, MOCI 20/2016 and GR71/2019, HUAWEI CLOUD, as an electronic system operator, actively responds to and fulfills its obligations. It adopts the following privacy protection mechanisms and technologies to comply with the requirements of Indonesia privacy regulations.

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
Personal Data Collection	<ol style="list-style-type: none">1. Collect personal data in a manner that is limited, specific, lawful, and fair.2. Prior to the personal data collection, notify personal data subjects and obtain their consent, unless other legal reasons are present.	<ol style="list-style-type: none">1. HUAWEI CLOUD follows the basic principles of privacy protection of being lawful, fair, transparent, and data minimization. HUAWEI CLOUD will evaluate business needs before collecting personal data, collect only the minimum personal data required by the business, clarify the type of personal data collected, and select the appropriate and legal personal data collection basis.2. When a customer registers for an account, HUAWEI CLOUD

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		clearly informs customers of the types of personal data to be collected, purposes, and legal basis of personal data collection and processing in the Privacy Policy Statement , so that customers can clearly understand related personal data processing activities and agree to them. 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 notices 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.
Personal Data Processing	<ol style="list-style-type: none">1. The processing of personal data is carried out in accordance with the objectives disclosed to the personal data subject.2. The processing of personal data is performed in an accurate, complete, non-misleading, up-to-date, accountable manner. Protect personal data from loss, misuse, unauthorized access, alteration, destruction or disclosure.	<ol style="list-style-type: none">1. HUAWEI CLOUD clearly informs customers of the purposes of personal data processing in the Privacy Policy Statement and collects and processes personal data based on the purposes disclosed in the Privacy Policy Statement. HUAWEI CLOUD regularly conducts Privacy Impact Assessments for products and services that involve personal data in order to prevent the collection and processing of personal data in products and services beyond the scope required for their actual purposes.2. HUAWEI CLOUD attaches great importance to and takes appropriate physical, technical, and organizational measures to protect the security, accuracy, and integrity of personal data. For details about the protection measures taken by HUAWEI CLOUD, see the Privacy Policy

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		<p>Statement.</p> <p>3. HUAWEI CLOUD has obtained multiple certifications in relation to privacy compliance international standard, including ISO 27701, ISO 29151, ISO 27018, BS 10012, the audit report of SOC2 Type 1 privacy principle, and etc. Customers can also understand personal data security controls within HUAWEI CLOUD's environment through HUAWEI CLOUD security reports or certifications.</p>
Protection of Personal Data Subject's Rights	The personal data subjects' rights shall be protected during data processing. Personal data subjects shall be entitled to confidentiality of their personal data, filing complaints in the context of personal data dispute resolution with respect to failure in the protection of their personal data, updating or correcting, having access to and deleting their personal data, as well as the right to withdraw the consent.	In the Privacy Policy Statement , HUAWEI CLOUD clearly informs data subjects of their privacy rights, such as the right to access, correct, delete, object, restrict processing, portability, consent withdrawal, and complaints to regulators. HUAWEI CLOUD provides customers with convenient channels for exercising data subjects' rights. When a data subject submits a data subject's rights request to HUAWEI CLOUD, HUAWEI CLOUD will respond to the data subject's rights request in a timely manner.
Data Retention	Destroy personal data within the retention period or as required by regulations.	HUAWEI CLOUD clearly informs customers of the purposes of personal data processing in the Privacy Policy Statement . Unless otherwise required by laws or customers, HUAWEI CLOUD will retain personal data for a period of time that is necessary to achieve the processing purposes described in the Privacy Policy Statement . (The retention period of personal data may vary depending on the processing purpose and service). In addition, unless otherwise specified by applicable laws and regulations, HUAWEI CLOUD will anonymize or delete unnecessary personal data after the storage period expires after the customer deregisters the HUAWEI CLOUD account.

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
Notice of Personal Data Breaches	Electronic systems operators must provide written notice to personal data subjects when the providers fail to protect the data's confidentiality and must inform the personal data subjects of the potential damage from the breach. If the breach may cause the personal data subject harm, the electronic systems operator must confirm that the personal data subject received the breach notification. In the event of a serious breach, electronic systems operators must immediately secure the data and notify law enforcement and the Ministry of Communications and Information Technology (MOCI).	<p>HUAWEI CLOUD has set up a 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.</p> <p>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.</p> <p>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 regulatory filings will be conducted in accordance with local regulations.</p>
Certification	Obtain the necessary electronic system certification as required by laws and regulations.	HUAWEI CLOUD has passed internationally recognized certifications, including ISO27001 Information Security Management System Certification and CSA STAR Cloud Security International Gold Certification. Refer to 6. HUAWEI CLOUD Privacy Protection related Certifications for more information.
Processing Activity Records	Electronic system operators should provide audit track records on all activities of the electronic system managed by them.	<p>HUAWEI CLOUD retains activity records for privacy management activities:</p> <ul style="list-style-type: none">• A Privacy Impact Assessment will be performed before the service becomes available. The types of

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
		<p>personal data, collection purpose of personal data and retention period of personal data will be listed in the assessment record.</p> <ul style="list-style-type: none">• During the service's daily operation and maintenance, in accordance with the requirements of the regulations, retain the information related to personal data subjects' right requests and responses, and the operation log of implementing security measures.
Providing a Contact Person	A contact person, who is easily contacted by personal data subjects for the management of their personal data, should be provided.	Currently, HUAWEI CLOUD has set up a data protection officer. If you have any questions, comments, suggestions, etc., the customer can contact the Data Protection Officer at the email address provided in the Privacy Policy Statement .
Data Localization	Electronic system operators for public purposes should store and manage relevant electronic systems and electronic data in the territory of Indonesia, unless the domestically available technology is insufficient. Electronic system operators for private purposes may manage, process or store electronic system and electronic data outside the jurisdiction of Indonesia. The operator must allow the relevant authority and law enforcement agency to supervise it, including allowing the authority and law enforcement agency to access the electronic system and electronic data.	Based on HUAWEI CLOUD 's overall business plan and design, HUAWEI CLOUD has built a region in Indonesia. HUAWEI CLOUD services are divided by region. A region is the physical location where a customer's data is stored. HUAWEI CLOUD will never transfer data between regions without the customer's explicit approval.
Data Cross-Border Transfer	If electronic system operators need to transfer any personal data generated by government, regional governments, or individuals or entities residing in Indonesia outside of Indonesia, they must undergo a coordination process with	HUAWEI CLOUD will communicate with MOCI about the personal data transfer implementation plan before transferring personal data within Indonesia outside of Indonesia.

Basic Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD	Measures Taken by HUAWEI CLOUD
	MOCL.	

5

How HUAWEI CLOUD Supports Customers to Comply with Indonesia Privacy Regulations

5.1 Customers' Privacy Protection Responsibilities

When the customer use HUAWEI CLOUD services or applications as personal data controller to process personal data included in their content data, the customer may be subject to the PDP Law. In this case, the customer shall assume the privacy protection responsibilities required by the PDP Law. In addition, HUAWEI CLOUD will do its best to help the customer achieve privacy security.

Basic Obligations of the Regulations	Customer's Privacy Protection Responsibilities (As the data controller)	HUAWEI CLOUD Service Support Provided to Customers
Personal Data Collection	<ol style="list-style-type: none">1. Collect personal data in a manner that is limited, specific, lawful, and fair.2. Prior to the personal data collection, notify personal data subjects and obtain their consent, unless other legal reasons are present.	<p>HUAWEI CLOUD only processes data according to the customer's instructions. The customer shall collect personal data in a fair and transparent manner and ensure that the purpose is appropriate. The customer shall not use personal data for purposes other than those agreed upon. In addition, the basis, purpose, scope, accuracy, and data retention period of content data collection are managed by the customer.</p> <p>HUAWEI CLOUD will inform customers of the types of personal data to be collected and processed in the service statements of some products and services to help customers formulate their privacy policies more accurately and meet the</p>

		basic principles of fair, legal, and transparent data protection.
Personal Data Processing	<ol style="list-style-type: none"> 1. The processing of personal data is carried out in accordance with the objectives disclosed to the personal data subject. 2. The processing of personal data is performed in an accurate, complete, non-misleading, up-to-date, accountable manner. Protect personal data from loss, misuse, unauthorized access, alteration, destruction or disclosure. 	<p>HUAWEI CLOUD only processes data according to the customer's instructions. The customer shall collect personal data in a fair and transparent manner and ensure that the purpose is appropriate. The customer shall not use personal data for purposes other than those agreed upon. In addition, the basis, purpose, scope, accuracy, and data retention period of content data collection are managed by the customer.</p> <p>HUAWEI CLOUD provides customers with various data security and privacy protection tools. For example, Database Security Service (DBSS) provides customers with functions such as user behavior discovery and audit, sensitive data protection, and real-time alarm, ensuring the security and integrity of customers' cloud data. Identity and Access Management (IAM) provides identity authentication and permission management functions to manage user accounts (such as employee accounts, system accounts, and applications) and control the operation permissions of these users on resources to prevent unauthorized access. Customers can use the data security and privacy protection tools provided by HUAWEI CLOUD to meet their requirements and ensure the security of personal data.</p>
Protection of Personal Data Subject's Rights	The personal data subject's rights shall be protected during data processing. Personal data subjects shall be entitled to confidentiality of their personal data, filing complaints in the context of personal data dispute resolution with respect to	HUAWEI CLOUD will take proactive measures to assist customers in meeting their obligations under applicable data protection laws and assist customers in responding to data subjects' rights requests.

	failure in the protection of their personal data, updating or correcting, having access to and deleting their personal data, as well as the right to withdraw the consent.	When a data subject submits a data subject's rights request to HUAWEI CLOUD, HUAWEI CLOUD will notify the customer of the request in a timely manner and respond only according to the customer's instructions.
Data Retention	Destroy personal data within the retention period or as required by regulations.	Customers should develop a mechanism for deleting personal data in content data and delete specified data through cloud database products. Most HUAWEI CLOUD products or services provide the data deletion function. Customers can proactively delete customer content data to minimize the data retention period.
Notice of Personal Data Breaches	In the event of a personal data breach, notify the data subject and the supervisory authority in writing within 72 hours, and inform them of the personal data that has been breached, the time and manner of the personal data breach, and the remedial measures taken by the personal data controller in response to the personal data breach.	In the event of a personal data breach, HUAWEI CLOUD will immediately notify the customer through relevant channels (including but not limited to emails and SMS messages) after discovering the personal data breach and assist the customer in handling the personal data breach to comply with relevant laws and regulations.
Data Protection Impact Assessment	A data protection impact assessment shall be carried out if the processing operation may pose a high risk to the rights and freedoms of the personal data subject due to its nature, scope, context and purpose.	Customers have full control over their content data. HUAWEI CLOUD only processes and collects data according to customers' instructions or requirements, and does not manage the purpose of collecting content data.
Data Security	Appropriate technical and organizational measures shall be taken to protect data security.	HUAWEI CLOUD provides customers with multiple privacy protection technologies and services. For example, Identity and Access Management (IAM) can be used to prevent unauthorized modification of content data by implementing appropriate user management, identity authentication, and fine-

		grained access control on cloud resources. Customers can use Data Encryption Workshop (DEW) to centrally manage keys throughout the lifecycle to ensure data integrity during storage. With the products and services provided by HUAWEI CLOUD, customers can better carry out personal data protection activities based on service requirements to meet their own requirements.
Records of Processing Activities	All personal data processing activities shall be recorded.	HUAWEI CLOUD provides Log Tank Service (LTS) and Cloud Trace Service (CTS) to help customers quickly collect and analyze logs and detect privacy risks in a timely manner. The LTS provides log collection, real-time query, and storage functions, helping users easily cope with daily operation and O&M scenarios such as real-time log collection, query, and analysis. Users can use the LTS to keep personal information operation records. CTS provides operation records of resources under cloud accounts for security analysis, compliance audit, and problem locating. You can configure CTS object storage to synchronize operation records to CTS in real time for a longer period of time.
DPO	A DPO shall be appointed to fulfill personal data protection responsibilities.	-
Cross-border Transfer of Data	Personal data may be transferred to another country only if: ensure that the level of personal data protection in the country where the controller and/or the personal data processor receiving the transfer is located is not lower than the legal level; ensure that personal data is adequately protected if the foregoing conditions are not met; If the preceding two conditions are not met, the consent	HUAWEI CLOUD points out in the Data Processing Addendum that the region for processing customer data can be specified by the customer. HUAWEI CLOUD can transfer customer data from the region selected by the customer only in the following cases: <ul style="list-style-type: none">● Necessary to provide the

	of the personal data subject shall be obtained.	<p>services required by the customer, especially to investigate security incidents or violations of this Agreement.</p> <ul style="list-style-type: none">● Necessary to comply with applicable laws and regulations or binding orders issued by courts or competent public authorities. <p>HUAWEI CLOUD also states in the Data Processing Addendum that relevant parties should recognize that applicable data protection laws do not require a data transfer agreement when transferring customer data to a country that is deemed to have an adequate level of protection. When transferring customer data to another third country, HUAWEI CLOUD will sign a data transfer agreement with the recipient located in the third country.</p> <p>HUAWEI CLOUD has a dedicated team to communicate with customers. Customers can contact HUAWEI CLOUD to obtain information such as the destination country name and recipient name.</p> <p>It is recommended that the customer evaluate the level of personal data protection provided by the countries involved in the data transfer and use a formal mechanism to transfer personal data across borders.</p>
--	---	---

Basic Obligations of the Regulations	Customer's Privacy Protection Responsibilities (As the data processor)	HUAWEI CLOUD Service Support Provided to Customers
Obligations of Personal Data	1. Processing personal data in accordance with the instructions of the personal	HUAWEI CLOUD provides customers with multiple privacy protection

Processors	<p>data controller.</p> <ol style="list-style-type: none">2. Maintaining the accuracy, completeness and consistency of personal data.3. Maintaining the security and confidentiality of personal data to prevent unauthorized processing and unauthorized access.4. Documenting personal data processing activities.	<p>technologies and services. For example, Identity and Access Management (IAM) can be used to prevent unauthorized modification of content data by implementing appropriate user management, identity authentication, and fine-grained access control on cloud resources. Customers can use Data Encryption Workshop (DEW) to centrally manage keys throughout the lifecycle to ensure data integrity during storage. With the products and services provided by HUAWEI CLOUD, customers can better carry out personal data protection activities based on service requirements to meet their own requirements.</p> <p>HUAWEI CLOUD provides Log Tank Service (LTS) and Cloud Trace Service (CTS) to help customers quickly collect and analyze logs and detect privacy risks in a timely manner. The LTS provides log collection, real-time query, and storage functions, helping users easily cope with daily operation and O&M scenarios such as real-time log collection, query, and analysis. Users can use the LTS to keep personal information operation records. CTS provides operation records of resources under cloud accounts for security analysis, compliance audit, and problem locating. You can configure CTS object storage to synchronize operation records to CTS in real time for a longer period of time.</p>
-------------------	--	--

When customers use HUAWEI CLOUD services to provide services subject to EIT, MOCI 20/2016 and GR71/2019 to other electronic system users, HUAWEI CLOUD will help customers fulfill the corresponding obligations.

Basic Obligations of the Regulations	Customer's Privacy Protection Responsibilities	HUAWEI CLOUD Service Support Provided to Customers
Personal Data Collection	<ol style="list-style-type: none"> 1. Collect personal data in a manner that is limited, specific, lawful, and fair. 2. Prior to the personal data collection, notify personal data owners and obtain their consent, unless other legal reasons are present. 	<p>HUAWEI CLOUD only processes data according to the customer's instructions. The customer shall collect personal data in a fair and transparent manner and ensure that the purpose is appropriate. The customer shall not use personal data for purposes other than those agreed upon. In addition, the basis, purpose, scope, accuracy, and data retention period of content data collection are managed by the customer.</p> <p>HUAWEI CLOUD will inform customers of the types of personal data to be collected and processed in the service statements of some products and services to help customers formulate their privacy policies more accurately and meet the basic principles of fair, legal, and transparent data protection. In addition, customers should develop a mechanism for deleting personal data in content data and delete specified data through cloud database products. Most HUAWEI CLOUD products or services provide the data deletion function. Customers can proactively delete customer content data to minimize the data retention time.</p>
Personal Data Processing	<ol style="list-style-type: none"> 1. The processing of personal data is carried out in accordance with the objectives disclosed to the personal data subject. 2. The processing of personal data is performed in an accurate, complete, non-misleading, up-to-date, accountable manner. Protect personal data from loss, misuse, unauthorized access, alteration, destruction or disclosure. 	<p>HUAWEI CLOUD only processes data according to the customer's instructions. The customer shall collect personal data in a fair and transparent manner and ensure that the purpose is appropriate. The customer shall not use personal data for purposes other than those agreed upon. In addition, the basis, purpose, scope, accuracy, and data retention</p>

		<p>period of content data collection are managed by the customer.</p> <p>HUAWEI CLOUD provides customers with various data security and privacy protection tools. For example, Database Security Service (DBSS) provides customers with functions such as user behavior discovery and audit, sensitive data protection, and real-time alarm, ensuring the security and integrity of customers' cloud data. Identity and Access Management (IAM) provides identity authentication and permission management functions to manage user accounts (such as employee accounts, system accounts, and applications) and control the operation permissions of these users on resources to prevent unauthorized access. Customers can use the data security and privacy protection tools provided by HUAWEI CLOUD to meet their requirements and ensure the security of personal data.</p>
Protection of Personal Data Subject's Rights	The personal data subjects' rights shall be protected during data processing. Personal data subjects shall be entitled to confidentiality of their personal data, filing complaints in the context of personal data dispute resolution with respect to failure in the protection of their personal data, updating or correcting, having access to and deleting their personal data, as well as the right to withdraw the consent.	HUAWEI CLOUD will take proactive measures to assist customers in meeting their obligations under applicable data protection laws and assist customers in responding to data subjects' rights requests. When a data subject submits a data subject's rights request to HUAWEI CLOUD, HUAWEI CLOUD will notify the customer of the request in a timely manner and respond only according to the customer's instructions.
Data Retention	Destroy personal data within the retention period or as required by regulations.	Customers should develop a mechanism for deleting personal data in content data and delete specified data through cloud database products. Most HUAWEI

		CLOUD products or services provide the data deletion function. Customers can proactively delete customer content data to minimize the data retention period.
Notice of Personal Data Breaches	Electronic systems operators must provide written notice to personal data subjects when the providers fail to protect the data's confidentiality and must inform the personal data subjects of the potential damage from the breach. If the breach may cause the personal data subject harm, the electronic systems operator must confirm that the personal data subject received the breach notification. In the event of a serious breach, electronic systems operators must immediately secure the data and notify law enforcement and the Ministry of Communications and Information Technology (MOCI).	In the event of a personal data breach, HUAWEI CLOUD will immediately notify the customer through relevant channels (including but not limited to emails and SMS messages) after discovering the personal data breach and assist the customer in handling the personal data breach to comply with relevant laws and regulations.
Certification	Obtain the necessary electronic system certification as required by laws and regulations.	HUAWEI CLOUD has passed internationally recognized certifications, including ISO27001 Information Security Management System Certification and CSA STAR Cloud Security International Gold Certification. Refer to 6. HUAWEI CLOUD Privacy Protection related Certifications for more information.
Processing Activity Records	Electronic system operators should provide audit track records on all activities of the electronic system managed by them.	HUAWEI CLOUD provides Log Tank Service (LTS) and Cloud Trace Service (CTS) to help customers quickly collect and analyze logs and detect privacy risks in a timely manner. The LTS provides log collection, real-time query, and storage functions, helping users easily cope with daily operation and O&M scenarios such as real-time log collection, query, and analysis. Users can use the LTS to keep personal information operation records. CTS provides operation records of resources

		under cloud accounts for security analysis, compliance audit, and problem locating. You can configure CTS object storage to synchronize operation records to CTS in real time for a longer period of time.
Providing a Contact Person	A contact person, who is easily contacted by personal data subjects for the management of their personal data, should be provided.	-
Data Localization	Electronic system operators for public purposes should store and manage relevant electronic systems and electronic data in the territory of Indonesia, unless the domestically available technology is insufficient. Electronic system operators for private purposes may manage, process or store electronic system and electronic data outside the jurisdiction of Indonesia. The operator must allow the relevant authority and law enforcement agency to supervise it, including allowing the authority and law enforcement agency to access the electronic system and electronic data.	Based on Huawei Cloud's overall business plan and design, Huawei Cloud has built a region in Indonesia. Huawei Cloud services are divided by region. A region is the physical location where a customer's data is stored. Huawei Cloud will never transfer data between regions without the customer's explicit approval.
Data Cross-Border Transfer	If electronic system operators need to transfer any personal data generated by government, regional governments, or individuals or entities residing in Indonesia outside of Indonesia, they must undergo a coordination process with MOCI.	HUAWEI CLOUD has a dedicated team to communicate with customers. Customers can contact HUAWEI CLOUD to obtain information such as the destination country name and recipient name. It is recommended that the customer evaluate the level of personal data protection provided by the countries involved in the data transfer and use a formal mechanism to transfer personal data across borders.

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

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

- **Management and Deployment of Products**

Product	Description	Corresponding Core Requirements and Control Measures
Identity and Access Management (IAM)	<p>Identity and Access Management (IAM) provides identity authentication and permissions management. With IAM, customers can create users for employees, applications, or systems in their organization, and control the users' permissions on owned resources.</p> <p>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.</p>	<p>Personal data collection</p> <p>Personal data processing</p> <p>Data Security</p>
Cloud Trace Service (CTS)	<p>Customers can review logs to perform security analysis, review compliance, and locate issues, etc.</p> <p>Customers can configure CTS object storage service to save operation records to CTS in real time and for a long period, protect the right to know of personal data subjects, and enable quick searching.</p>	<p>Processing activity records</p> <p>Protection of personal data subject's rights</p> <p>Data Security</p>
Cloud Eye Service (CES)	<p>Providing customers with a multidimensional monitoring platform for elastic cloud servers, bandwidth and other resources.</p> <p>Through CES, customers can have a comprehensive understanding of HUAWEI CLOUD resources usage and business operations status, and respond to alarms in time to ensure business continuity.</p>	<p>Personal data processing</p> <p>Notice of personal data breaches</p> <p>Data Security</p>

Product	Description	Corresponding Core Requirements and Control Measures
Log Tank Service (LTS)	<p>Providing functions such as log collection, real-time query and storage, which can be used to make real-time decision analysis, improve the efficiency of log processing, and help customers to cope with daily operations and maintenance scenarios such as real-time logs collection and query analysis without development's requirements.</p> <p>Customers can keep records of operations on personal data through LTS to guarantee the personal data subjects' right to know.</p>	<p>Personal data processing</p> <p>Notice of personal data breaches</p> <p>Data Security</p>

- **Security Products**

Product	Description	Corresponding Core Requirements and Control Measures
Database Security Service (DBSS)	<p>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.</p> <p>Customers can use DBSS to detect potential risks and ensure the security of their databases.</p>	<p>Personal Data Processing</p> <p>Data Security</p>
Data Encryption Workshop (DEW)	<p>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.</p> <p>Customers can use DEW for centralized key lifecycle management to ensure the integrity of data storage procedures.</p>	<p>Personal Data Processing</p> <p>Data Security</p>

Web Application Firewall (WAF)	<p>Web Application Firewall (WAF) can conduct multi-dimensional detection and protection of website traffic, combining with deep machine learning to identify malicious requests, protect against unknown threats, and block common attacks such as SQL injection or cross-site scripting.</p> <p>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.</p>	Personal Data Processing Data Security
Advanced Anti-DDoS (AAD)	<p>Advanced Anti-DDoS (AAD) is a value-added security defense service that defends against large volumetric DDoS attacks on Internet servers.</p> <p>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.</p>	Personal Data Processing Data Security
Data Security Center (DSC)	<p>Data Security Center (DSC) is a new-generation cloud-native data security platform that provides basic data security capabilities which helps identify, classify, and mask sensitive or confidential data</p> <p>Customers can use DSC to integrate the status of each phase of the data security lifecycle to build a cloud service panorama to protect the security of data collection, storage, transmission, use, exchange, and destruction.</p>	Personal Data Processing Data Security
Cloud Certificate Manager (CCM)	<p>Cloud Certificate Manager (CCM) is a cloud service that provides one-stop lifecycle management of digital certificates including SSL certificate and private certificate.</p> <p>Customers can use CCM to improve the confidentiality and security of SSL certificates and private certificates, improve the security of access and transmission channels, and reduce the risk of unauthorized data intrusion, access, or theft during transmission and access.</p>	Personal Data Processing Data Security

- **Network Products**

Product	Description	Corresponding Core Requirements and Control Measures
Virtual Private Network (VPN)	Virtual Private Network (VPN) establishes a flexible, scalable IPsec encrypted communication channel between customers' local data center and their VPC on HUAWEI CLOUD. Customers can build a flexible and scalable hybrid cloud computing environment, and improve their security posture with encryption of the communication channel.	Personal Data Processing Data Security
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.	Personal Data Processing Data Security

- **Storage Products**

Product	Description	Corresponding Core Requirements and Control Measures
Volume Backup Service (VBS)	Volume Backup Service (VBS) creates online permanent incremental backup for cloud hard disk, automatically encrypts the backup disk data, and can restore the data to any backup point to enhance data availability. VBS can reduce the possibility of virus attack, human error deletion as well as hardware or software failure, protect data security and reliability, and reduce the risk of data tampering.	Personal Data Processing Data Security
Cloud Server Backup Service (CSBS)	Cloud Server Backup Service (CSBS) can simultaneously create a consistent online backup of multiple cloud drives	Personal Data Processing Data Security

Product	Description	Corresponding Core Requirements and Control Measures
	<p>within the cloud server.</p> <p>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.</p>	

6

HUAWEI CLOUD Privacy Protection Related Certifications

HUAWEI CLOUD inherits Huawei's comprehensive management system and leverages its experience in IT system construction and operation, actively managing and continuously improving the development, operation and maintenance of cloud services. To date, HUAWEI CLOUD has received a number of global, regional, and industry-specific security compliance certifications ensuring the security and compliance of businesses deployed by cloud service customers.

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

Example of Huawei Cloud Partial Standard Certification:

Certification	Description
ISO27001:2022	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
ISO27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that HUAWEI CLOUD has achieved internationally recognized best practices in information security management.
ISO27018:2019	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection

Certification	Description
	management system and is in the global leading position in data security management.
TL 9000& ISO 9001	<p>ISO 9001 defines a set of core standards for quality management systems (QMS). It can be used to certify that an organization has the ability to provide products that meet customer needs as well as applicable regulatory requirements.</p> <p>TL 9000 is a quality management system built on ISO 9001 and designed specifically for the communications industry by the QuEST Forum (a global association of ICT service providers and suppliers). It defines quality management system specifications for ICT products and service providers and includes all the requirements of ISO 9001. Any future changes to ISO9001 will also cause changes to TL 9000.</p> <p>Huawei Cloud has earned ISO 9001/TL 9000 certification, which certifies its ability to provide you with faster, better, and more cost-effective cloud services.</p>
ISO 20000-1:2018	ISO 20000 is an international recognized information technology Service Management System (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers(CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO22301:2019	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that

Certification	Description
	entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
CSA STAR Certification	The Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider, developed CSA STAR certification. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
ISO27701:2019	ISO 27701 specifics requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
ISO29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD' s implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
PCI DSS	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover,

Certification	Description
	MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
PCI 3DS	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that HUAWEI CLOUD complies with security standards in the process, flow, and personnel management of the 3D protocol execution environment.
ISO 27799:2016	ISO/IEC 27799 provides guidelines on how organizations in the healthcare industry can better protect the confidentiality, integrity, traceability, and availability of personal health information. Huawei Cloud is the world's first cloud service provider to earn ISO/IEC 27799 certification. This certifies Huawei Cloud's deep understanding of intelligent applications for the healthcare industry, and its ability to protect the security of personal health information.
ISO 27034	ISO/IEC 27034 is the first ISO standard for secure programs and frameworks. It clearly defines risks in application systems and provides guidance to assist organizations in integrating security into their processes. ISO/IEC 27034 provides a way for organizations to verify their own product security and make security a competitive edge. This standard also outlines a compliance framework at the application layer for global cloud service providers, promoting the security of the R&D process, applications, and the cloud. Huawei Cloud is the world's first cloud service provider to obtain ISO/IEC 27034 certification. This marks a big step forward for

Certification	Description
	Huawei Cloud governance and compliance.
SOC Audit Report	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers.

7 Conclusion

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

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

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

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

8 Version History

Date	Version	Description
2024-7	2.2	Routine update
2023-12	2.1	Routine update
2023-7	2.0	Routine update
2022-4	1.1	Routine update
2021-1	1.0	First release