

HUAWEI CLOUD Compliance with Kenya Privacy Protection Regulations

Issue	1.0
Date	2023-02-24



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. 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



HUAWEI and other Huawei trademarks are the property 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 Contents..... 1

2 Overview..... 2

2.1 Scope of Application..... 2

2.2 Purpose of Publication..... 2

2.3 Basic Definition..... 2

3 Privacy Protection Responsibilities..... 5

4 Overview of Kenyan Privacy Laws and Regulations..... 7

4.1 Background of Kenyan Privacy Protection Laws and Regulations..... 7

4.2 Role Division and Basic Obligations..... 7

4.3 HUAWEI CLOUD's Role under Kenya Privacy Laws and Regulations..... 9

5 How HUAWEI CLOUD is Satisfying the Requirements of Kenyan Privacy Protection Laws and Regulations..... 10

5.1 HUAWEI CLOUD Privacy Commitment..... 10

5.2 HUAWEI CLOUD Basic Privacy Protection Principles..... 10

5.3 4HUAWEI CLOUD's Compliance Measures in Response to Kenya Data Protection Act and Data Protection (General) Regulations..... 11

6 How HUAWEI CLOUD Supports Customers to Comply with Kenyan Privacy Protection Laws and Regulations..... 31

6.1 Customers' Privacy Protection Responsibilities under Kenya Data Protection Act and Data Protection (General) Regulations..... 31

6.2 How HUAWEI CLOUD Products and Services Help Customers Implementing Content Data Privacy and Security..... 42

7 HUAWEI CLOUD Privacy Protection Related Certifications..... 48

8 Conclusion..... 50

9 Version History..... 51

1 Contents

2 Overview

2.1 Scope of Application

The information provided in this document applies to HUAWEI CLOUD and all its products and services in Kenya.

2.2 Purpose of Publication

This document is intended to help customers understand:

1. HUAWEI CLOUD's privacy protection responsibility model;
2. Kenya privacy related legal requirements;
3. HUAWEI CLOUD's responsibilities on compliance with Kenya 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 Kenya privacy regulations, as specified in the responsibility model;
6. How to leverage HUAWEI CLOUD's security products and services to achieve privacy compliance.

2.3 Basic Definition

- **Personal Data**
Means any information relating to an identified or identifiable natural person.
- **Data subject**
Means an identified or identifiable natural person who is the subject of personal data.
- **Data Controller**

Means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.

- **Data Processor**

Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

- **Personal Data Processing**

Means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as (a) collection, recording, organisation, structuring; (b) storage, adaptation or alteration; (c) retrieval, consultation or use; (d) disclosure by transmission, dissemination, or otherwise making available; or (e) alignment or combination, restriction, erasure or destruction.

- **Personal Data Breach**

Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **Pseudonymisation**

Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

- **Anonymisation**

Means the removal of personal identifiers from personal data so that the data subject is no longer identifiable.

- **Biometric Data**

Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

- **Sensitive Personal Data**

Means personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition.

- **Third Party**

Means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

- **HUAWEI CLOUD**

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

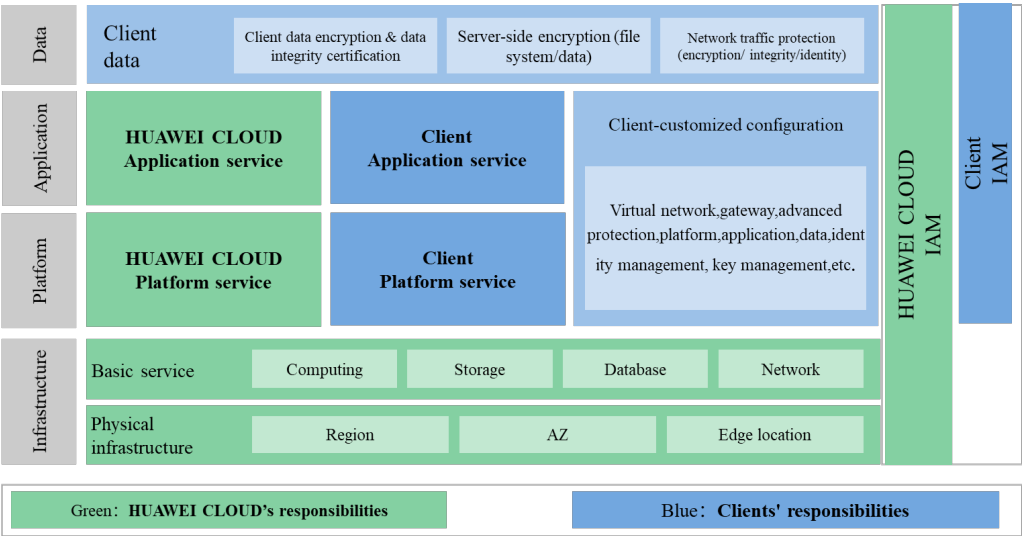
- **Customer**

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

3 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 effort 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 3-1 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 should 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 personal data subject requests: Tenants should 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 tenant should notify both regulatory authorities and personal data subjects, and take adequate actions in accordance with regulatory requirements.

4 Overview of Kenyan Privacy Laws and Regulations

4.1 Background of Kenyan Privacy Protection Laws and Regulations

On November 11, 2019, the Parliament of Kenya promulgated **Data Protection Act, No. 24 of 2019 (DPA)**, which clarifies the regulatory responsibilities of security authorities and establishes a collaborative governance system for data security. The Act contains the obligations of data controllers and data processors, as well as the principles of personal data protection and requirements for overseas data transmission. On March 14, 2022, the Parliament of Kenya promulgated **Data Protection (General) Regulations 2021**, which aims to clarify the scope of the principles and obligations specified in DPA, and specify the relevant compliance requirements such as the power to authorize data subjects, the restrictions on the commercial use of personal data, the obligations of data controllers and data processors, the elements of data protection, and the transfer of personal data overseas.

4.2 Role Division and Basic Obligations

Kenya **DPA** defines three roles: data controller, data processor, and data subject.

Data subject is an identified or identifiable natural person who is the subject of personal data. They have the right to be informed of the use to which their personal data is to be put, to access their personal data in custody of data controller or data processor, to object to the processing of all or part of their personal data, to correction of false or misleading data and to deletion of false or misleading data about them.

Data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Data controller's basic obligations are heavier than those of a data processor, including:

- **Personal Data Collection:** A data controller or data processor shall collect personal data directly from the data subject. Under certain circumstances, personal data may be collected indirectly.
- **Fully Inform before Data Collection:** A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject.
- **Principles of Personal Data Processing:** Processed in accordance with the right to privacy of the data subject; processed lawfully, fairly and in a transparent manner in relation to any data subject; collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes; adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed; collected only where a valid explanation is provided whenever information relating to family or private affairs is required; accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.
- **Protect Data Subjects' Rights:** A data subject has a right to be informed of the use to which their personal data is to be put; to access their personal data in custody of data controller or data processor; to object to the processing of all or part of their personal data; to correction of false or misleading data; and to deletion of false or misleading data about them.
- **Lawful Processing of Personal Data:** A data controller or data processor shall not process personal data, unless the data subject consents to the processing for one or more specified purposes; or the processing is necessary.
- **Data Retention:** A data controller or data processor shall ensure that personal data is kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed; shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained.
- **Notice of Personal Data Breaches:** Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach; communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established; Where the notification to the Data Commissioner is not made within seventy-two hours, the notification shall be accompanied by reasons for the delay.
- **Data Protection Impact Assessment:** Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.
- **Data Processing for Commercial Purposes:** A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person has sought and obtained express consent from a data subject; or is authorised to do so under any written law and the data

subject has been informed of such use when collecting the data from the data subject.

- **Data Security:** Every data controller or data processor shall implement appropriate technical and organisational measures to insure data security.
- **Data Cross-Border Transfer:** A data controller or data processor may transfer personal data to another country only where the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data; the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws; the transfer is necessary. The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.

4.3 HUAWEI CLOUD's Role under Kenya Privacy Laws and 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 processing personal data included in content data, HUAWEI CLOUD is generally regarded as the personal data processor. HUAWEI CLOUD acts as the personal 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 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 Kenya privacy protection laws and regulations requirements 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 data 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 controller of the personal data, and maintains records of data processing operations.

5

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

5.1 HUAWEI CLOUD Privacy Commitment

HUAWEI CLOUD has placed cyber security and privacy protection as top priorities. 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.

5.2 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 Limitation**

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

- **Data Minimization**

When HUAWEI CLOUD processes personal data, personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for

which the data is processed. Personal data will be anonymized or pseudonymized to the extent possible to reduce the risks for 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.

- **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.

5.3 4HUAWEI CLOUD's Compliance Measures in Response to Kenya Data Protection Act and Data Protection (General) Regulations

Based on the characteristics of HUAWEI CLOUD's business and in accordance with the requirements of the Kenya Data Protection Act and Data Protection (General) Regulations, HUAWEI CLOUD, as a legal entity that processes personal data, assumes two roles of controller and data processor of personal data in different scenarios. HUAWEI CLOUD actively responds and fulfills its obligations by adopting the following personal data protection mechanisms and technologies to comply with the requirements of the Kenya Data Protection Act and Data Protection (General) Regulations.

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Personal Data Collection	<p>A data controller or data processor shall collect personal data directly from the data subject.</p> <p>A data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined.</p>	<p>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.</p> <p>In the Privacy Statement, HUAWEI CLOUD informs customers that personal data is collected only for clear and explicit purposes, such as account registration, account security, and real-name authentication. All personal data collected has specific purposes. In addition, personal data is the minimum scope necessary to provide a specific service. All collection purposes and uses are disclosed in the privacy statement. Customers can choose whether to agree to the privacy statement.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Fully Inform before Data Collection	<p>A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of:</p> <ul style="list-style-type: none"> • the rights of data subject; • the fact that personal data is being collected; • the purpose for which the personal data is being collected; • the third parties whose personal data has been or will be transferred to, including details of safeguards adopted; • the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data; • a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data; • the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and • the consequences if any, where the data subject fails to provide all or any part of the requested data. 	<p>Before HUAWEI CLOUD collects customer personal data, if the customer needs to collect personal data during the interaction between the customer and HUAWEI CLOUD, In the Privacy Statement, HUAWEI CLOUD will proactively and fully inform customers of the rights of data subjects, types and purposes of collected personal data, how to process personal data, how to transfer personal data, retention period of personal data, how to share personal data, and how to process personal data. Transfer, how to take appropriate physical, organizational and technical measures to protect personal data, personal information, etc.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Principles of Personal Data Processing	<p>Every data controller or data processor shall ensure that personal data is:</p> <ul style="list-style-type: none"> • processed in accordance with the right to privacy of the data subject; • processed lawfully, fairly and in a transparent manner in relation to any data subject; • collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes; • adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed; • collected only where a valid explanation is provided whenever information relating to family or private affairs is required; • accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; • kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and • not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject. 	<p>In the process of customer interaction with HUAWEI CLOUD, if the customer's personal data is to be collected, Huawei Cloud will actively and fully inform the customer of the type, purpose, processing method, retention period, how to transfer personal information, how to protect personal information and other contents in the Privacy Statement.</p> <p>HUAWEI CLOUD processes customers' personal data only in compliance with the agreement on personal data processing or use specified in the Privacy Statement, and does not involve further processing of customers' personal data that is not notified.</p> <p>Huawei Cloud ensures that the customer's personal data is complete, accurate, and not misleading, and is updated when necessary. According to the purpose of personal data processing, Huawei Cloud will take reasonable measures to ensure that inaccurate personal data is deleted or corrected in a timely manner. At the same time, appropriate technical or organizational measures will be taken to prevent personal data from accidental or illegal damage, loss, tampering, unauthorized access or disclosure according to existing technical capabilities, implementation</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
		<p>costs, privacy risk degree and probability.</p> <p>HUAWEI CLOUD provides a convenient channel for customers to exercise the rights of data owners. Customers can request to access and modify their incorrect or incomplete personal data in the Privacy Statement. HUAWEI CLOUD will provide customers with copies of the personal data they have queried after verifying the identity information of the requestor, or update, replace or revoke the incomplete or inaccurate information as requested.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Protect Data Subjects' Rights	<p>A data subject has a right:</p> <ul style="list-style-type: none"> • to be informed of the use to which their personal data is to be put; • to access their personal data in custody of data controller or data processor; • to object to the processing of all or part of their personal data; • to correction of false or misleading data; and • to deletion of false or misleading data about them. 	<p>Data subject rights: HUAWEI CLOUD will present the Privacy Statement to the customer when a customer registers an account. The Privacy Statement describes how HUAWEI CLOUD will collect and process the customer's personal data, the necessity of data collection, the consequences of refusing to provide the data, the purpose and processing method of data use, and the data receiving for data transmission. Party type, legal interests of the data controller or third party (if any), contact information of HUAWEI CLOUD and the data protection officer, and inform the data subject that the data subject has privacy rights such as access rights, correction rights, deletion or restriction rights, portability rights, and withdrawal of consent according to applicable laws and regulations.</p> <p>Personal Data Management Request: HUAWEI CLOUD provides a convenient channel for customers to exercise data owners' rights. Customers can initiate a request to access or modify incorrect or incomplete personal data on the privacy question page of personal data subjects' requests through the data subjects' rights request portal described in the Privacy Statement. HUAWEI CLOUD will</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
		<p>respond to the request within the legal period after verifying the identity of the requester. For example, provide a copy of the queried personal data to the customer, and update or change incomplete or inaccurate information according to the customer's request. Delete related personal data as requested by customers. Provide the customer with a copy of the queried personal data or update, replace, or cancel incomplete or inaccurate information as requested.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Lawful Processing of Personal Data	<p>A data controller or data processor shall not process personal data, unless</p> <ol style="list-style-type: none"> 1. the data subject consents to the processing for one or more specified purposes; or 2. the processing is necessary — <ul style="list-style-type: none"> • for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; • for compliance with any legal obligation to which the controller is subject; • in order to protect the vital interests of the data subject or another natural person; • for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; • the performance of any task carried out by a public authority; • for the exercise, by any person in the public interest, of any other functions of a public nature; • for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or 	<p>HUAWEI CLOUD collects and processes personal data based on the purposes disclosed in the Privacy 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.</p> <p>When a customer registers for an account, HUAWEI CLOUD will provide the Privacy Statement and obtain the customer's consent. 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. HUAWEI CLOUD processes customers' personal data only as specified in the signed user agreement and privacy policy statement. HUAWEI CLOUD processes personal data for the</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
	<ul style="list-style-type: none"> for the purpose of historical, statistical, journalistic, literature and art or scientific research. <p>Further processing of personal data shall be in accordance with the purpose of collection.</p>	<p>purposes disclosed in the Privacy Statement, such as complying with and enforcing applicable laws or regulatory requirements or industry standards, or fulfilling obligations under contracts signed with customers. necessary to protect the rights or property of HUAWEI CLOUD, our customers, and/or the public.</p>
Data Retention	<p>A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is —</p> <ul style="list-style-type: none"> required or authorised by law; reasonably necessary for a lawful purpose; authorised or consented by the data subject; or for historical, statistical, journalistic literature and art or research purposes. <p>A data controller or data processor shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under sub-section 1 in a manner as may be specified at the expiry of the retention period.</p>	<p>HUAWEI CLOUD regularly audits the purposes of collecting, using and disclosing personal data.</p> <p>When personal data owners request to delete their personal data, HUAWEI CLOUD will respond to the rights of personal data owners with security processing such as anonymizing or deleting personal data, in addition to comply with the applicable laws and regulations.</p> <p>When customers cancel the HUAWEI CLOUD account, except to comply with applicable laws and regulations, HUAWEI CLOUD will anonymize or delete personal data that are no longer needed.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Notice of Personal Data Breaches	<ol style="list-style-type: none"> Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall: <ul style="list-style-type: none"> notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach; and subject to subsection 3, communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established. Where the notification to the Data Commissioner is not made within seventy-two hours, the notification shall be accompanied by reasons for the delay. Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller without delay and where reasonably practicable, within forty-eight hours of becoming aware of such breach. The data controller may delay or restrict communication referred to under subsection 1(b) as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body. 	<p>HUAWEI CLOUD has established a response process for responding to cyber security incidents to monitor potential cyber-attacks in a timely manner to prevent data breaches. If a data breach occurs, the 24/7 professional security incident response team is responsible for the execution of the emergency response plan, disclosure to the local regulatory authorities and customers within the time specified by laws and internal regulations, and records the incident through the log recording system.</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 owners' business, initiates the notification process according to the notification mechanism of security incidents, and notifies personal data owners 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</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
	<p>4. The notification and communication referred to under subsection 1 shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including:</p> <ul style="list-style-type: none"> • description of the nature of the data breach; • description of the measures that the data controller or data processor intends to take or has taken to address the data breach; • recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise; • where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and • the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained. <p>1. The communication of a breach to the data subject shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data.</p> <p>2. Where and to the extent that it is not possible to</p>	<p>recommended for customers. In addition, necessary regulatory filings will be conducted in accordance with local regulations.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
	<p>provide all the information mentioned in subsection 5 at the same time, the information may be provided in phases without undue delay.</p> <p>3. The data controller shall record the following information in relation to a personal data breach:</p> <ul style="list-style-type: none"> • the facts relating to the breach; • its effects; and • the remedial action taken. 	

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Data Protection Impact Assessment	Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.	To effectively identify and control privacy risks, HUAWEI CLOUD conducts extensive privacy risk analysis and management in various cloud services. Service scenarios that pose high risks to the rights and freedoms of data subjects. For example, high-risk services or cloud services, such as user profiling and prediction, processing of data related to criminal convictions or crimes, processing of biometric data or genetic data, processing of health data, and large-scale processing of data. 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.

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Data Processing for Commercial Purposes	<p>A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person —</p> <p>(a) has sought and obtained express consent from a data subject; or</p> <p>(b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.</p> <p>A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.</p>	<p>Purpose notification: HUAWEI CLOUD collects customers' personal data necessary for providing services only after obtaining customers' consent and processes the personal data within the purpose specified in the Privacy Statement. For example, performance of obligations under contracts with customers; Send service information that may be of interest to the customer; Invite customers to participate in HUAWEI CLOUD activities (including promotion activities), market surveys, or satisfaction surveys. or send marketing information to customers.</p> <p>Obtain the Explicit Consent of the Customer: When registering on the HUAWEI CLOUD official website, a customer can choose whether to allow HUAWEI CLOUD to use their personal data for marketing. Marketing information is pushed to the customer only after obtaining the customer's consent.</p> <p>Right to Withdraw Consent: HUAWEI CLOUD provides various configuration options on the official website. Customers can set the types and modes of receiving messages based on their preferences. If the customer does not want to receive marketing information, the customer can adjust the</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
		information receiving settings on the “HUAWEI CLOUD official website - User Center”.

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Data Security	<p>Every data controller or data processor shall implement appropriate technical and organisational measures;</p> <p>Identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;</p> <p>Establish and maintain appropriate safeguards against the identified risks;</p> <p>The pseudonymisation and encryption of personal data;</p> <p>The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;</p> <p>Verify that the safeguards are effectively implemented;</p> <p>Ensure that the safeguards are continually updated in response to new risks or deficiencies.</p>	<p>Organizational Security Measures: HUAWEI has set up a global cyber security and privacy protection officer who is responsible for the formulation and implementation of HUAWEI's privacy protection policy . HUAWEI CLOUD has set up a team of privacy protection experts, including privacy protection experts, legal personnel, and network and information security professionals, to provide professional support for HUAWEI CLOUD privacy protection strategy and practice. For countries and regions where it operates, HUAWEI CLOUD assigns dedicated legal and privacy protection personnel to help HUAWEI CLOUD implement local activities in compliance with applicable privacy laws and regulations. HUAWEI CLOUD has established a privacy protection governance framework covering all businesses, and through a series of privacy protection processes, to support business activities to meet privacy protection requirements, such as data owners' rights protection, emergency response to data breaches, and personal data retention, etc. HUAWEI CLOUD retains complete records of any personal data processing activities performed by HUAWEI CLOUD. Every service lists</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
		<p>the type of data owners, the type of personal data, the collection purpose, the transfer of personal data, retention period and security measures etc. through conducting privacy impact assessments.</p> <p>Data access and operation control:</p> <ul style="list-style-type: none"> • Authentication: strict password policy and multi-factor authentication are adopted; • Permission management: role-based access control and permission management for operation and maintenance personnel is implemented; • Data storage and transfer: encryption is adopted for sensitive data; • Risk monitoring: logging and auditing of data processing is adopted to monitor and audit the access to the key systems. <p>Backup and Recovery: HUAWEI CLOUD has a backup strategy. It will regularly back up personal data, and regularly test the effectiveness of the backup of personal data in the system, and keep records of the backup test.</p> <p>High availability: In addition to the high availability infrastructure, data redundancy and backup, Huawei Cloud also has a formal business continuity plan (BCP) and conducts BCP drills periodically. This plan,</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
		<p>which applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud services and safeguards customers' service and data security. Huawei Cloud also develops a DR plan, which it uses to perform regular testing.</p> <p>Security Certification: 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, ISO 27018 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.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Data Cross-Border Transfer	<p>A data controller or data processor may transfer personal data to another country only where:</p> <p>the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;</p> <p>the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;</p> <p>the transfer is necessary —</p> <p>(a) for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request;</p> <p>(b) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;</p> <p>(c) for any matter of public interest;</p> <p>(d) for the establishment, exercise or defence of a legal claim;</p> <p>(e) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or</p>	<p>HUAWEI CLOUD has established data centers in multiple countries around the world. When cross-border data transmission is required during O&M, HUAWEI CLOUD complies with local privacy protection laws and regulations and passes strict internal review. If cross-border data transfer is performed after a data transfer agreement is signed or the explicit consent of the data subject is obtained, ensure that personal data is processed in a legal, proper, and transparent manner.</p> <p>HUAWEI CLOUD has set up a team of privacy experts to estimate the level of personal data protection provided by the countries involved in data transfer. For the countries and regions where it operates, HUAWEI CLOUD also has fulltime legal and privacy protection personnel to help HUAWEI CLOUD take necessary measures in accordance with applicable privacy laws and regulations.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to HUAWEI CLOUD (As the personal data controller)	Measures Taken by HUAWEI CLOUD
	<p>(f) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.</p> <p>The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.</p>	

6

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

6.1 Customers' Privacy Protection Responsibilities under Kenya Data Protection Act and Data Protection (General) Regulations

When the customer is the data controller and HUAWEI CLOUD provides assistance in processing personal data in the customer's content data, or when the customer is the data administrator but use HUAWEI CLOUD's services to process personal data, the customer is likely to fall within the jurisdiction of Kenyan Privacy Protection Laws and Regulations and relevant regulations. If so, customers should meet the compliance requirements of Kenyan Privacy Protection Laws and Regulations and relevant regulations, and HUAWEI CLOUD will provide compliance support to customers in the following areas.

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Personal Data Collection	<p>A data controller or data processor shall collect personal data directly from the data subject.</p> <p>A data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined.</p>	HUAWEI CLOUD only follows the customer's instructions regarding data processing. The purpose and scope of content data collection are managed by the customer.

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Fully Inform before Data Collection	<p>A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of:</p> <ul style="list-style-type: none"> • the rights of data subject; • the fact that personal data is being collected; • the purpose for which the personal data is being collected; • the third parties whose personal data has been or will be transferred to, including details of safeguards adopted; • the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data; • a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data; • the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and • the consequences if any, where the data subject fails to provide all or any part of the requested data. 	Some of HUAWEI CLOUD's products and services provide customers with the ability to embed privacy statements and record related operations to help them implement policies that inform their personal data owners about personal data processing.

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Principles of Personal Data Processing	<p>Every data controller or data processor shall ensure that personal data is:</p> <ul style="list-style-type: none"> • processed in accordance with the right to privacy of the data subject; • processed lawfully, fairly and in a transparent manner in relation to any data subject; • collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes; • adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed; • collected only where a valid explanation is provided whenever information relating to family or private affairs is required; • accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; • kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and • not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject. 	<p>HUAWEI CLOUD only follows the customer's instructions regarding data processing. The scope or any further processing for the content data is managed by the customer or added in the contract.</p> <p>HUAWEI CLOUD only follows the customer's instructions or the contract signed with the customer regarding data storing or processing. HUAWEI CLOUD will not transfer personal data to any third party without the customer's consent.</p> <p>HUAWEI CLOUD provides customers with a variety of data security and privacy protection tools, such as vulnerability scanning services and Web application firewall to help customers ensure that their content data is accurate and not tampered with.</p> <p>Customers should form the deletion mechanism of personal data in content data and can delete specific data through cloud database products.</p> <p>Data deletion function is provided in most HUAWEI CLOUD products or services enabling customers to delete content data.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Protect Data Subjects' Rights	<p>A data subject has a right:</p> <ul style="list-style-type: none"> • to be informed of the use to which their personal data is to be put; • to access their personal data in custody of data controller or data processor; • to object to the processing of all or part of their personal data; • to correction of false or misleading data; and • to deletion of false or misleading data about them. 	<p>HUAWEI CLOUD has set up a dedicated team to support and communicate with customers. Customers can seek help from HUAWEI CLOUD through the service ticket.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Lawful Processing of Personal Data	<p>A data controller or data processor shall not process personal data, unless</p> <ol style="list-style-type: none"> 1. the data subject consents to the processing for one or more specified purposes; or 2. the processing is necessary — <ul style="list-style-type: none"> • for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; • for compliance with any legal obligation to which the controller is subject; • in order to protect the vital interests of the data subject or another natural person; • for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; • the performance of any task carried out by a public authority; • for the exercise, by any person in the public interest, of any other functions of a public nature; • for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or 	<p>HUAWEI CLOUD only process data in accordance with customers' instructions. Customers should collect personal data through the principle of fairness and transparency and ensure the appropriateness of the purpose. Customers should not use personal data for non-contractual purposes.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
	<ul style="list-style-type: none"> for the purpose of historical, statistical, journalistic, literature and art or scientific research. <p>Further processing of personal data shall be in accordance with the purpose of collection.</p>	
Data Retention	<p>A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is —</p> <ul style="list-style-type: none"> required or authorised by law; reasonably necessary for a lawful purpose; authorised or consented by the data subject; or for historical, statistical, journalistic literature and art or research purposes. <p>A data controller or data processor shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under sub-section 1 in a manner as may be specified at the expiry of the retention period.</p>	Data deletion function is provided in most HUAWEI CLOUD products or services, enabling customers to delete content data.

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Notice of Personal Data Breaches	<ol style="list-style-type: none"> Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall: <ul style="list-style-type: none"> notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach; and subject to subsection 3, communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established. Where the notification to the Data Commissioner is not made within seventy-two hours, the notification shall be accompanied by reasons for the delay. Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller without delay and where reasonably practicable, within forty-eight hours of becoming aware of such breach. The data controller may delay or restrict communication referred to under subsection 1(b) as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body.。 	<p>HUAWEI CLOUD has developed a comprehensive personal data breach management system. Relevant personnel will analyze the impact of the incident based on the process. If the incident has affected or will affect the cloud service customer, HUAWEI CLOUD will start a notification mechanism to notify the customer of the incident. The notification content includes but is not limited to the incident description, cause, impact, measures taken by HUAWEI CLOUD, and measures recommended by the customer.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
	<p>4. The notification and communication referred to under subsection 1 shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including:</p> <ul style="list-style-type: none"> • description of the nature of the data breach; • description of the measures that the data controller or data processor intends to take or has taken to address the data breach; • recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise; • where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and • the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained. <p>1. The communication of a breach to the data subject shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data.</p> <p>2. Where and to the extent that it is not possible to</p>	

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
	<p>provide all the information mentioned in subsection 5 at the same time, the information may be provided in phases without undue delay.</p> <p>3. The data controller shall record the following information in relation to a personal data breach:</p> <ul style="list-style-type: none"> • the facts relating to the breach; • its effects; and • the remedial action taken. 	
Data Protection Impact Assessment	Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.	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 Processing for Commercial Purposes	<p>A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person —</p> <p>(a) has sought and obtained express consent from a data subject; or</p> <p>(b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.</p> <p>A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.</p>	Some of HUAWEI CLOUD products and services provide clients with the ability to embed privacy statements and record related operations. Customers can inform data owners in the privacy statement that their personal data will be used for marketing purposes.

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Data Security	<p>Every data controller or data processor shall implement appropriate technical and organisational measures;</p> <p>Identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;</p> <p>Establish and maintain appropriate safeguards against the identified risks;</p> <p>The pseudonymisation and encryption of personal data;</p> <p>The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;</p> <p>Verify that the safeguards are effectively implemented;</p> <p>Ensure that the safeguards are continually updated in response to new risks or deficiencies.</p>	<p>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.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
Data Cross-Border Transfer	<p>A data controller or data processor may transfer personal data to another country only where:</p> <p>the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;</p> <p>the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;</p> <p>the transfer is necessary —</p> <p>(a) for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request;</p> <p>(b) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;</p> <p>(c) for any matter of public interest;</p> <p>(d) for the establishment, exercise or defence of a legal claim;</p> <p>(e) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or</p>	<p>When the customer proactively transmits data across borders, it is recommended that the customer evaluate the level of personal data protection provided by the countries involved in the data transmission and use a formal mechanism to transmit personal data across borders.</p> <p>HUAWEI CLOUD, as a data processor, complies with local privacy protection laws and regulations and passes strict internal review when cross-border data transmission is required during O&M. If cross-border data transfer is performed after a data transfer agreement is signed or data subjects' explicit consent is obtained, ensure that personal data is processed in a legal, proper, and transparent manner.</p>

Basic Legal Obligations of the Regulations	Specific Requirements Applicable to Customer (As the personal data controller)	Measures Taken by HUAWEI CLOUD
	<p>(f) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.</p> <p>The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.</p>	

6.2 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 Kenyan Privacy Protection Laws and 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 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>Data Protection Act (Article 28, 26, 30, 34, 38, 39, 40, 41, 42)</p> <p>Data Protection (General) Regulations (Article 5, 7, 10, 11, 12, 19, 24, 43)</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 data owners, and enable quick searching.</p>	<p>Data Protection Act (Article 25, 26, 30, 34, 38, 39, 40)</p> <p>Data Protection (General) Regulations (Article 5, 7, 10, 11, 12, 19, 21, 28, 46)</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>Data Protection Act (Article 25, 29, 30, 43)</p> <p>Data Protection (General) Regulations (Article 5, 21, 28, 37, 38, 46)</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 data owners' right to know.</p>	<p>Principles of Personal Data Processing</p> <p>Personal Data Breaches</p> <p>Data Security</p> <p>Protect Data Subjects' Rights</p> <p>Data Protection Act (Article 25, 26, 34, 38, 39, 40, 43)</p> <p>Data Protection (General) Regulations (Article 7, 10, 11, 12, 19, 21, 28, 37, 38, 46)</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>Data Protection Act (Article 41, 42)</p> <p>Data Protection (General) Regulations (Article 24, 43)</p>

<p>Data Encryption Workshop(DEW)</p>	<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>Data Protection Act (Article 25, 41, 42)</p> <p>Data Protection (General) Regulations (Article 21, 28, 24, 43, 46)</p>
<p>Web Application Firewall(WAF)</p>	<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>	<p>Data Protection Act (Article 25, 41, 42)</p> <p>Data Protection (General) Regulations (Article 21, 28, 24, 43, 46)</p>
<p>Advanced Anti-DDoS (AAD)</p>	<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>	<p>Data Protection Act (Article 41, 42)</p> <p>Data Protection (General) Regulations (Article 24, 43)</p>

- **Network Products**

Product	Description	Corresponding Core Requirements and Control Measures
Virtual Private Network (VPN)	<p>Virtual Private Network (VPN) establishes a flexible, scalable IPsec encrypted communication channel between customers' local data center and their VPC on HUAWEI CLOUD.</p> <p>Customers can build a flexible and scalable hybrid cloud computing environment, and improve their security posture with encryption of the communication channel.</p>	<p>Data Protection Act (Article 41, 42)</p> <p>Data Protection (General) Regulations (Article 24, 43)</p>
Virtual Private Cloud (VPC)	<p>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.</p> <p>VPC is the customer's private network on the cloud, with 100% isolation from other customers, enhancing the data security on the cloud.</p>	<p>Data Protection Act (Article 41, 42)</p> <p>Data Protection (General) Regulations (Article 24, 43)</p>

- **Storage Products**

Product	Description	Corresponding Core Requirements and Control Measures
Volume Backup Service (VBS)	<p>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.</p> <p>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.</p>	<p>Data Protection Act (Article 41, 42)</p> <p>Data Protection (General) Regulations (Article 24, 43)</p>

Product	Description	Corresponding Core Requirements and Control Measures
Cloud Server Backup Service (CSBS)	Cloud Server Backup Service (CSBS) can simultaneously create a consistent online backup of multiple cloud drives within the cloud server. CSBS can reduce the possibility of virus attack, human error deletion as well as hardware or software failure, protect data security and reliability, and reduce the risk of data tampering.	Data Protection Act (Article 41, 42) Data Protection (General) Regulations (Article 24, 43)

7 HUAWEI CLOUD Privacy Protection Related Certifications

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

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

Privacy Related Standard Certification:

- **ISO 27701**
Privacy information management system certification. The ISO 27701 certification shows that HUAWEI CLOUD has established a solid management system related to data privacy protection.
- **ISO 29151**
International practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
- **ISO 27018**
International code of conduct focused on the protection of personal data in Cloud. The adoption of ISO 27018 indicates that HUAWEI CLOUD has met the requirements of an internationally recognized personal data protection measures of public cloud platform, and can guarantee the security of customers' personal data.
- **BS 10012**
Personal data management system standard issued by the British Standards Institute (BSI). The BS 10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
- **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, SOC 2 Type I 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
- ISO 27799 Health Information Security Management System Certification
- CSA STAR Cloud Security International Gold Certification
- PCI DSS Third-Party Payment Industry Data Security Standard Certification
- International Common Criteria (CC) EAL3+ Security Assessment Standard
- Management & Operations Stamp of Approval (M&O Program)
- NIST Cybersecurity Framework
- Payment Card Industry Three Domain Secure Certification (PCI 3DS)

Regional Security Certifications:

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

8 Conclusion

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

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

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

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

9

Version History

Date	Version	Description
Feb 2023	1.0	First release