



**Malaysia Personal Data Protection Act 2010 (Act 709)
and PDP Amendment Act (2024)
Compliance Whitepaper**



Contents

1. Legal Notices	3
2. Overview	4
Objective	4
Scope	4
Key definitions	4
3. Alibaba Cloud's Approach to Data Protection and Security	6
4. Overview of Malaysia's PDPA	8
4.1. Data Controller's Obligations	9
4.2. Data Processor's Obligations	10
5. How Alibaba Cloud Helps Customers Meet the Requirements of Malaysia's PDPA	12
Customer's Responsibility	12
Alibaba Cloud Response	12
6. How Alibaba Cloud Products and Services Help Customers to Meet the Requirements of Malaysia's PDPA	17
6.1 Resource Access Management (RAM)	17
6.2 ActionTrail	17
6.3 CloudMonitor	18
6.4 Log Service	19
6.5 Key Management Service (KMS)	19
6.6 Web Application Firewall (WAF)	20
6.7 Security Center	20
6.8 Anti-DDoS	21
6.9 Virtual Private Cloud (VPC)	21
6.10 VPN Gateway	22
6.11 Block Storage	22
6.12 Object Storage Service (OSS)	23
7. Alibaba Cloud Security & Privacy Protection Related Certifications	24
8. Conclusion and Summary	28

1. Legal Notices

Alibaba Cloud reminds you to carefully read through and completely understand all content in this section before you read or use this document. If you read or use this document, it is considered that you have identified and accepted all contents declared in this section.

1. You shall download this document from the official website of Alibaba Cloud or other channels authorized by Alibaba Cloud. This document is only intended for legal and compliant business activities. The contents in this document are confidential, so you shall have the liability of confidentiality. You shall not use or disclose all or part of contents in this document to any third party without written permission from Alibaba Cloud.
2. Any sector, company, or individual shall not extract, translate, reproduce, spread, or publicize, in any method or any channel, all or part of the contents in this document without written permission from Alibaba Cloud.
3. This document may be subject to change without notice due to product upgrades, adjustment, and other reasons. Alibaba Cloud reserves the right to modify the contents in this document without notice and to publish the document in an authorized channel from time to time. You shall focus on the version changes of this document, download and get the updated version from channels authorized by Alibaba Cloud.
4. This document is only intended for product and service reference. Alibaba Cloud provides this document for current products and services with current functions, which may be subject to change. Alibaba Cloud makes the best efforts to provide an appropriate introduction and operation guide on the basis of current technology, but Alibaba Cloud does not explicitly or implicitly guarantee the accuracy, completeness, suitability, and reliability of this document. Alibaba Cloud does not take any legal liability for any error or loss caused by downloading, using, or putting trust in this document by any sectors, company, or individuals. In any case, Alibaba Cloud does not take any legal liability for any indirect, consequential, punitive, occasional, incidental, or penalized damage, including profit loss due to use of or trust to this document (even if Alibaba Cloud has notified you it is possible to cause this kind of damage).
5. All content, including, but not limited to images, architecture design, page layout, description text, and its intellectual property (including but not limited to trademarks, patents, copyrights, and business secrets) in this document are owned by Alibaba Cloud and/or its affiliates. You shall not use, modify, copy, publicize, change, spread, release, or publish the content from the official website, products, or programs of Alibaba Cloud without the written permission from Alibaba Cloud and/or its affiliates. Nobody shall use, publicize, or reproduce the name of Alibaba Cloud for any marketing, advertisement, promotion, or other purpose (including, but not limited to, a separate or combined form to use the name, brand, logo, pattern, title, product or service name, domain name, illustrated label, symbol, sign, or similar description that may mislead readers and let them identify it comes from Alibaba Cloud and/or its affiliates, of or from Alibaba Cloud, Aliyun, Wanwang, and/or its affiliates) without the written permission from Alibaba Cloud.
6. If you find any error or mistake in this document, directly contact Alibaba Cloud.

2. Overview

Objective

The purpose of this whitepaper is to inform our customers about Malaysia's Personal Data Protection Act 2010 (Act 709, "PDPA"), as amended by the Personal Data Protection (Amendment) Act 2024 (Act A1727), and demonstrate how Alibaba Cloud leverages its global security infrastructure and privacy-first capabilities to protect customer data. Alibaba Cloud is dedicated to supporting our customers in Malaysia as they migrate and manage workloads, ensuring their use of Alibaba Cloud tools and services is consistent with PDPA mandates.

This document outlines our comprehensive data protection features and provides a detailed mapping of our services to the regulatory requirements. Please be advised that while Alibaba Cloud provides the tools for compliance, we do not provide legal advice; customers should consult with their own legal counsel regarding their specific compliance obligations.

Scope

The information provided in this document only applies to Alibaba Cloud and its products and services available in Malaysia.

Key definitions

The definitions used in this whitepaper are based on the terminology established in the PDPA:

Personal Data	Any information processed in commercial transactions that relates directly or indirectly to a data subject, who is identified or identifiable from the information or from that and other information in the possession of a data controller. This includes sensitive personal data and expressions of opinion about the data subject.
Sensitive Personal Data	Personal data consisting of information on the physical or mental health or condition of a data subject, political opinions, religious beliefs or other beliefs of a similar nature, the commission or alleged commission of any offence, biometric data, or any other personal data as determined by the Minister.
Biometric Data	Any personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a person.
Data Controller	A person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor. Previously termed "data user" under the original Act 709; renamed by the 2024 Amendment.
Data Processor	Any person, other than an employee of the data controller, who processes personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes (Section 4, Act 709).
Data Subject	An individual who is the subject of the personal data, and shall not include a deceased individual (Section 3(f), Act A1727 – amended to exclude deceased individuals).
Personal Data Breach	Any breach of personal data, loss of personal data, misuse of personal data, or unauthorized access of personal data.

Data Protection Officer (DPO)	One or more persons appointed by a data controller (and data processor, where applicable) who shall be accountable for the organisation's compliance with the PDPA.
Commissioner	The Personal Data Protection Commissioner appointed under Section 47 of Act 709.
Commercial Transaction	Any transaction of a commercial nature, whether contractual or not, which includes any matter relating to the supply or exchange of goods or services, agency, investment, financing, banking and insurance, but does not include a credit reporting business.
Customer	A registered user of Alibaba Cloud.
Customer Business Data	The data generated when Customers use Alibaba Cloud applications to develop their business. It also refers to the data that Customers process, store, upload, download, or distribute by using Alibaba Cloud services.

3. Alibaba Cloud's Approach to Data Protection and Security

Data security and user privacy are the top priorities of Alibaba Cloud. Alibaba Cloud is mindful of its role under the PDPA and is committed to ensuring that its duties and obligations under the PDPA are fully complied with. Alibaba Cloud is committed to building a public, open, and secure cloud computing service platform and aims to turn cloud computing into a state-of-the-art computing infrastructure by investing heavily in technical innovation to continually improve the computing capabilities and economies of scale of its services.

Alibaba Cloud strives to provide customers with consistent, reliable, secure, and compliant cloud computing services, helping customers ensure the confidentiality, integrity, and availability of their systems and data in a manner consistent with the requirements of the PDPA.

Shared Security Responsibilities

The security of applications built on Alibaba Cloud is the joint responsibility of Alibaba Cloud and the customers. Alibaba Cloud is responsible for the security of the underlying cloud service platform and providing security services and capabilities to customers, while customers are responsible for the security of applications built based on Alibaba Cloud services.

Security Responsibilities of Customers			
User Account Security	User Business Security	User Security Monitoring & Operation	Alibaba Cloud Security Services & Ecosystem
	User Application Security		
	User Data Security		
	User Infrastructure Security		
Security Responsibilities of the Cloud Platform			
Identity & Access Control	Cloud Product Security	Security Monitoring & Operation	Security Capabilities of the Alibaba Cloud Platform
	Visualization Security		
	Hardware Security		
	Physical Security		

Alibaba Cloud must ensure the security of infrastructure (including but not limited to data centres deployed across regions and zones, and Alibaba backbone networks), physical devices (including computing, storage, and network devices), virtualization solutions, and cloud products running on top of the Apsara distributed cloud OS. Alibaba Cloud is also responsible for identity management and access control, monitoring, and operations of the platform to provide customers with a highly available and secure cloud service platform.

Customers maintain full control over the lifecycle of their member content on Alibaba Cloud, including its creation, usage, storage duration, and eventual destruction. They determine

where the content is stored, selecting the type of storage and its geographic location. Financial entities also define the secured state of their content, including its format, structure, and whether it is masked, anonymized, or encrypted. Alibaba Cloud supports this by offering robust encryption for member content both in transit and at rest, while also providing the option for customers to manage their own encryption keys. Additionally, customers oversee access to their member content and control access to Alibaba Cloud services and resources through the management of users, groups, permissions, and credentials.

Customers must configure and use cloud products based on security best practices, and build applications on the securely configured cloud products. Alibaba Cloud offers Alibaba Cloud Security, which leverages years of expertise in attack prevention technologies to help customers protect their applications and systems. Customers can choose to use Alibaba Cloud Security or any third-party security products in the Alibaba Cloud security ecosystem to protect their applications and business systems.

Alibaba Cloud employs a shared security responsibility model between itself and its customers, where Alibaba Cloud secures the cloud platform and provides integrated cloud security products and capabilities to customers. This relieves much of the underlying security burdens while allowing customers to focus more on their core business needs. Combined with the right IT governance and controls within the customer, these should understandably help alleviate regulatory concerns relating to the utilisation of cloud services.

As Alibaba Cloud does not have visibility into or knowledge of what customers are uploading onto its network, including whether or not that data is deemed subject to the PDPA, customers are ultimately responsible for their own compliance with the PDPA and related regulations.

4. Overview of Malaysia's PDPA

Malaysia's Personal Data Protection Act 2010 (Act 709, "PDPA") was passed by the Malaysian Parliament on 2 June 2010 and came into force on 15 November 2013. It governs the collection, use, and disclosure of personal data in commercial transactions and requires certain entities to register their processing activities. It also grants rights to data subjects, including rights to access, correction, consent withdrawal, and objection to certain types of processing. Violations of the law may result in criminal penalties, including fines or imprisonment.

The PDPA applies to the processing of personal data in commercial transactions by persons established in Malaysia or by persons not established in Malaysia but who use equipment in Malaysia for processing purposes (other than transit). The PDPA does not apply to the Federal Government and State Governments. Most private organisations engaged in commercial transactions are subject to the law, with the exception of credit reporting agency businesses.

Unlike many global data protection laws which govern the data processing activities of both controllers and processors, the original PDPA imposed obligations primarily on "data users" (now termed "data controllers"). However, the 2024 Amendment significantly expanded the obligations of data processors, now requiring them to independently comply with the Security Principle and to appoint Data Protection Officers.

To operationalize these statutory requirements, this whitepaper is designed to be read in conjunction with the relevant regulatory guidelines issued by the Department of Personal Data Protection (JPDP), including the DBN Guidelines, DPO Guidelines, and Cross-Border Personal Data Transfer (CBPDT) Guidelines.

Important Note: As data protection regulations and administrative guidelines continue to evolve, organizations should actively monitor official announcements from the JPDP and consult the latest published guidelines and circulars to ensure ongoing compliance.

The Seven Personal Data Protection Principles

At the core of the PDPA are seven Personal Data Protection Principles that govern the processing of personal data:

Processing of Personal Data		
General Principle (Section 6)		Personal data may not be processed without the data subject's consent (or where an exemption applies). Processing must be for a lawful purpose directly related to the data controller's activity, necessary for that purpose, and not excessive.
Notice and Choice Principle (Section 7)		Data controllers must provide written notice (in Bahasa Malaysia and English) to data subjects about the processing of their personal data, including the purpose, source, rights, third-party disclosures, and choices available.
Disclosure Principle (Section 8)		Personal data shall not be disclosed without consent for purposes other than those notified at collection, or to third parties other than those specified in the notice.

Security Principle (Section 9)	Data controllers (and now data processors, following the 2024 Amendment) must take practical steps to protect personal data from loss, misuse, modification, unauthorised access or disclosure, alteration, or destruction.
Retention Principle (Section 10)	Personal data shall not be kept longer than necessary for the fulfilment of the purpose for which it was collected. Data must be destroyed or permanently deleted when no longer required.
Data Integrity Principle (Section 11)	Data controllers must take reasonable steps to ensure personal data is accurate, complete, not misleading, and kept up-to-date.
Access Principle (Section 12)	Data subjects have the right to access their personal data held by a data controller and to request correction of inaccurate, incomplete, misleading, or outdated data.

4.1. Data Controller's Obligations

The PDPA mandates specific organizational and technical obligations for Data Controllers. Because Alibaba Cloud operates under a shared responsibility model, it is essential for customers to understand which regulatory tasks they must perform directly. The table below outlines the core obligations of the Controller:

Processing of Personal Data	
Legal Basis for Processing	Data Controllers must have a legal basis for processing personal data, such as consent, contractual necessity, legal obligation, vital interests, administration of justice, or functions conferred by law. Consent must be obtained before processing (excluding sensitive personal data subject to Section 40).
Purpose Limitation and Data Processing	Data Controllers must ensure personal data is processed for a lawful purpose directly related to their activity, that processing is necessary for or directly related to that purpose, and that data collected is adequate but not excessive.
Provision of Notice	Data Controllers must inform data subjects in writing (in both Bahasa Malaysia and English) of the processing of their personal data, including: purpose, source, right to access and correct, classes of third parties, choices to limit processing, and consequences of failure to supply data.
Disclosure Principle	Personal data shall not be disclosed without consent for purposes other than the original purpose or a directly related purpose, and shall not be disclosed to third parties other than those specified in the notice.
Data Integrity	Data Controllers must take reasonable steps to ensure personal data is accurate, complete, not misleading, and kept up-to-date.
Data Subject Rights	Data Controllers must facilitate: the right to access, right to correct, right to withdraw consent, right to prevent processing causing damage/distress, right to prevent direct marketing processing, and the new right to data portability.
Record of Processing Activity	Data Controllers must keep records of applications, notices, requests, or other information relating to personal data processed.

Data Retention and Erasure	Personal data shall not be kept longer than necessary. Data Controllers must take all reasonable steps to ensure data is destroyed or permanently deleted when no longer required.
Cross-Border Data Transfer	Data Controllers may transfer data outside Malaysia to jurisdictions with substantially similar laws or adequate protection. Data controllers may conduct Transfer Impact Assessment ("TIA") to review the relevant personal data protection law of the receiving country/ jurisdiction is equivalent to the Act. The 2024 Amendment also removed the prior Ministerial approval requirement. Transfers may also be permitted with consent, for contract performance, legal proceedings, vital interests, or public interest.
Appointment of DPO	Data Controllers must appoint one or more DPOs accountable for PDPA compliance and notify the Commissioner. The appointment does not discharge the Data Controller from its duties. Under the DPO Guidelines, mandatory appointment is triggered if the controller's processing involves: • Personal data of more than 20,000 data subjects. • Sensitive personal data (including financial transaction data) of more than 10,000 data subjects. • Activities requiring "regular and systematic monitoring" of personal data.
Registration	Data Controllers in specified classes must register with the Commissioner.
Data Security	
Privacy and Security Measures	Data Controllers must take practical steps to protect personal data from loss, misuse, modification, unauthorised access or disclosure, alteration or destruction. The 2024 Amendment extends this to data processors. Where processing is by a data processor, the Controller must ensure sufficient security guarantees.
Personal Data Breach Notification	Under the Data Breach Notification (DBN) Guidelines, Data Controllers must notify the Commissioner as soon as practicable and within 72 hours from the occurrence of the breach. If notification fails to be made to the Commissioner within 72 hours, a written notice detailing the reasons for the delay and providing supporting evidence must be submitted. Where significant harm is likely, the data subject must also be notified without unnecessary delay and within seven days of notifying the Commissioner.

4.2. Data Processor's Obligations

While the Data Controller holds primary accountability, the PDPA (as amended) now imposes specific statutory obligations directly upon Data Processors. As your cloud service provider, Alibaba Cloud acts as a Data Processor, carrying out processing activities strictly in accordance with the instructions provided by you – the Data Controller. The following table details the obligations of Data Processors under the PDPA:

Processing of Personal Data	
Compliance with Data Controller Instructions	Data Processors shall perform processing activities in accordance with the Data Controller's instructions.
Appointment of DPO	Where a data processor processes personal data on behalf of a data controller and meets the scale thresholds outlined in the Guidelines (e.g., managing data for controllers where the combined processing exceeds the 20,000 general subjects or 10,000 sensitive subjects threshold, or performing regular monitoring), the processor must appoint one or more DPOs.
Data Security	
Privacy, Security Measures, and Personal Data Breach	Data Processors must take practical steps to protect personal data from loss, misuse, modification, unauthorised access or disclosure, alteration or destruction. Data processors should implement measures to support the Data Controller in meeting their statutory notification windows for data breaches. Under the 2024 Amendment, data processors must now independently comply with the Security Principle, and must provide sufficient guarantees regarding technical and organisational security measures. To demonstrate objective compliance with these expanded statutory processor duties, Alibaba Cloud maintains the APEC Privacy Recognition for Processors (PRP) certification. This independent validation confirms that our operational policies, governance structures, and processing practices strictly align with regional privacy baselines for data processors, providing Data Controllers with verified compliance posture.

5. How Alibaba Cloud Helps Customers Meet the Requirements of Malaysia's PDPA

As a cloud service provider, Alibaba Cloud provides infrastructure and technical capabilities to our customers either for storage, processing, transfer, or deletion. When a customer acts as a Data Controller by utilizing Alibaba Cloud's products and services to process business data (which may contain personal data), Alibaba Cloud operates as a Data Processor. Under this shared responsibility model, customers maintain complete ownership and control over their data environments. Alibaba Cloud provides the underlying secure infrastructure to support customer's business operation, and only executes activities strictly according to the instructions provided by the Data Controller.

Data Protection Obligation	Customer's Responsibility	Alibaba Cloud Response
Processing of Personal Data		
Legal Basis For Processing Purpose Limitation And Data Processing Provision Of Notice	- Ensure that personal data is gathered, used, and disclosed lawfully. - Ensure that the data gathering, utilization, or sharing of personal data is restricted to the lawful purposes stated. - Customers are also required to disclose how they gather and handle personal data to data subjects in clear, plain Bahasa Malaysia and English language. - Establish a process for handling withdrawal of consent within 72 hours upon receipt.	- Customers maintain full control over the data you put into Alibaba Cloud's services, the cloud services you choose to use, how you use them, for what reasons and be able to access your data at any time. - Alibaba Cloud commits to processing data only as per the customer's instructions and the terms of the relevant contracts. - Alibaba Cloud's Data Processing Addendum (DPA) is entirely transparent to the public and can be found on our Legal Centre. - Alibaba Cloud provides the technical tools and capabilities (e.g., Management Console) allowing customers to access, manage, and delete their data at any time to facilitate compliance with subject rights and withdrawal requests.
Cross-Border Transfer	Customers should consider whether they should disclose to individuals (data subjects) the locations where they store or process their personal data and obtain consent relating to such locations from the relevant individuals if necessary.	- Alibaba Cloud provides Regions and Zones for customers to select from to host their data, which allows customers to store data in the Malaysia Region to meet data residency preferences. - Alibaba Cloud only stores and processes each customer's content in the Alibaba Cloud Region(s) that is chosen by the customer. Alibaba Cloud will not move customer content without the customer's consent. If a customer chooses to store data in more than one Region or copy or move content between Regions, that is solely the customer's choice. The customer will

Data Protection Obligation	Customer's Responsibility	Alibaba Cloud Response
		need to consider the legal requirements that apply to such operations, wherever content is moved and processed. - Alibaba Cloud applies the robust security measures to customer data wherever it is located. Our DPA clearly articulates our privacy and security commitments to our customer, which serves as an essential tool in assisting customers complete their Transfer Impact Assessments (TIAs) when necessary. - Furthermore, Alibaba Cloud's APEC Cross-Border Privacy Rules (CBPR) certification serves as an internationally recognized compliance blueprint. This enables Data Controllers to significantly streamline TIAs by leveraging a recognised framework for cross-border data flows within APEC economies.
Data subject rights (Access, Rectification, Erasure/Deletion, Restriction and Data Portability)	Establish procedures enabling data subjects to exercise rights of access, correction, erasure, consent withdrawal, and data portability. Portability requests are subject to technical feasibility and must be completed within the prescribed period.	- Customers may access their data on Alibaba Cloud at any time, Alibaba Cloud provides self-service tools, such as the Management Console, APIs and SDKs to allow customers to instantly access, extract, modify or delete the data you put onto cloud to fulfil the data subject's (customer's end users) requests. - Alibaba Cloud support customers in exporting their data in standard formats at any time. - Alibaba Cloud commits to process these actions solely as instructed by the customer. - If Alibaba Cloud receives a request from an individual (customer's end user) relating to their personal data, we will advise the requester to submit the request to you.
Records Of Processing Activity	Customers should maintain electronic records concerning its handling of personal data.	- Alibaba Cloud maintains electronic records concerning its handling of customer data. - Alibaba Cloud provides logging and auditing tools (such as ActionTrail and Cloud Config) that help customers track and document access and changes to their data, significantly assisting them in

Data Protection Obligation	Customer's Responsibility	Alibaba Cloud Response
		building their own ROPA for compliance audits.
Data Retention	Customers should remove any personal data they possess once its intended use has ended or when the data subjects withdraw consent.	- Alibaba Cloud will manage the retention, return, destruction, or deletion of customer data as per the terms of the contract. - The Alibaba Cloud management console allows customer to delete their data that has been uploaded to their cloud instance. - Customers can utilize Alibaba Cloud Object Storage Service (OSS), which provides robust data management tools including Lifecycle Management and Versioning. These features empower the Data Controller to enforce strict data retention schedules and perform permanent data destruction in alignment with PDPA requirements.
Appointment of Data Protection Officer	Appoint one or more DPOs accountable for PDPA compliance and notify the Commissioner.	- To assist customers' Data Protection Officers (DPOs) in executing their compliance responsibilities, Alibaba Cloud provides comprehensive documentation, compliance guides, and access to security certifications and audit reports through our Trust Centre to support DPOs in their oversight functions. - Alibaba Cloud has designated a DPO to oversee its processor-side compliance obligations under the Act. For regulatory transparency, Alibaba Cloud publishes the contact details of our DPO within our public Privacy Policy.
Data Protection Impact Assessment (DPIA)	Customers should conduct data protection impact assessment if the personal data processing has a high potential risk to the data subjects.	Alibaba Cloud recognizes that customers may need certain information in order to conduct a DPIA, our DPA articulates our privacy and security commitments to customers. In addition, customers can review Alibaba Cloud's security certifications and audit reports available in our Trust Centre.
Data Security		
Privacy and security measures	Customers should establish adequate security measures to safeguard personal data, including the correct	Alibaba Cloud manages the security of the underlying infrastructure. To demonstrate sufficient technical and organizational security measures for the data processing, Alibaba Cloud has

Data Protection Obligation	Customer's Responsibility	Alibaba Cloud Response
	configuration of cloud features.	published the latest version of our Alibaba Cloud Security Whitepaper describing our security methodology. The whitepaper covers various aspects, such as security policies, organizational security, compliance, data security, access control, personnel security, physical security, infrastructure security, systems and software development and maintenance, disaster recovery, and business continuity. • In addition, to demonstrate objective compliance with these expanded statutory processor duties, Alibaba Cloud maintains the APEC Privacy Recognition for Processors (PRP) certification. This independent validation confirms that our operational policies, governance structures, and processing practices strictly align with regional privacy baselines for data processors, providing Data Controllers with verified compliance posture. • Alibaba Cloud offers a comprehensive suite of security tools to help customers meet their PDPA obligations: ○ Identity and Access Management: RAM (Resource Access Management) for granular access control and ActionTrail for auditing user activities. ○ Network Security: VPC for network isolation, VPN Gateway for secure encrypted connections, and WAF (Web Application Firewall) and Anti-DDoS to protect against external cyber threats. ○ Data Protection: Key Management Service (KMS) for centralized encryption key management and Block Storage for secure, high-performance data-at-rest encryption. ○ Monitoring & Operations: Cloud Monitor and Simple Log Service for real-time visibility and forensics, and Security Centre for unified vulnerability management and threat detection.

Data Protection Obligation	Customer's Responsibility	Alibaba Cloud Response
		○ For more information, please refer to Section 6. How Alibaba Cloud Products and Services Help Customers to Meet the Requirements of Malaysia's PDPA
Personal data breach notification	• Establish and implement necessary policies and SOPs to address data breach incidents including but not limited to response, notification and remediation. • Notify the Commissioner as soon as practicable and notify affected data subjects where significant harm is likely.	• Alibaba Cloud ensures that information regarding significant developments affecting our ability to fulfil the services under the SLAs is accessible to you. • Additionally, Alibaba Cloud commits to promptly and without undue delay notify customers of any data incidents that would impact the customer. • Our incident detection team at Alibaba Cloud employs various tools to provide early indications of potential incidents. For details, please refer to the Alibaba Cloud Security Whitepaper. • Alibaba Cloud Security Centre serves as a centralized threat detection and response platform. It provides real-time monitoring, automated security alerts, and vulnerability scanning across the cloud environment. By leveraging its advanced threat intelligence and forensic capabilities, customers can rapidly identify potential data breaches, assess the impact, and gather the necessary information to meet the PDPA's strict notification timelines.

6. How Alibaba Cloud Products and Services Help Customers to Meet the Requirements of Malaysia's PDPA

6.1 Resource Access Management (RAM)

(a) Areas of compliance:

✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	RAM allows you to centrally manage access to Alibaba Cloud services and resources. You can use RAM to create and manage RAM users and user groups. You can also grant permissions to RAM users and user groups to control their access to cloud resources. Alibaba Cloud RAM is an identity and access control service which enables you to centrally manage your users (including employees, systems or applications) and securely control their access to your resources through permission levels. RAM thereby allows you to securely grant access permissions for Alibaba Cloud resources to only your selected high-privileged users, enterprise personnel and partners. This helps to ensure secure and appropriate usage of your cloud resources and protects from any unsolicited access to your account.
Type of Product	Cloud Management
Key Features	• Identity Management • SSO (Identity Federation) • Security Token Service • High Flexibility
Product Link	https://www.alibabacloud.com/product/ram

6.2 ActionTrail

(a) Areas of compliance:

✓ **Processing of Personal Data - Record of Processing Activity**

✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	A service that monitors and records the actions of your Alibaba Cloud account, including the access to and use of Alibaba Cloud services using the Alibaba Cloud Management console, calling API operations, or SDKs. ActionTrail tracks your Alibaba Cloud account actions and records them as events to facilitate auditing. ActionTrail allows you to deliver these events to the specified Log Service Logstores and Object Storage Service (OSS) buckets. You can also query and download the recorded events. Then, you can perform behaviour analysis, security analysis, and compliance auditing and track resource changes based on the events. ActionTrail records the actions you take in the Alibaba Cloud Management console or by calling API operations and the actions triggered by Alibaba Cloud services when these services assume

	RAM roles. When an action is taken, ActionTrail tracks and records the action in ten minutes.
Type of Product	Cloud Management
Key Features	• Records Events Generated in the Last 90 Days • Continuously Delivers Events • Collects Events Across Accounts
Product Link	https://www.alibabacloud.com/product/actiontrail

6.3 CloudMonitor

(a) Areas of compliance:

✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	Automate performance monitoring of all your web resources and applications in real time. CloudMonitor collects monitor metrics of Alibaba Cloud resources and custom metrics. The service can be used to detect the availability of your service and allows you to set alarms on specific metrics. CloudMonitor enables you to view and fully understand the usage of the cloud resources, and the status and health of your business, so that you can act promptly to ensure the availability of your application when an alarm is triggered.
Type of Product	O&M and Monitoring
Key Features	• Real-time Monitoring with Various Functionalities • End-to-end Monitoring Platform • Manage Applications by Group • Flexible and Accurate Alarms • Visual Dashboard
Product Link	https://www.alibabacloud.com/product/cloud-monitor

6.4 Log Service

(a) Areas of compliance:

- ✓ **Processing of Personal Data - Record of Processing Activity**
- ✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	An all-in-one service for log-type data. Log Service is a complete real-time data logging service that has been developed by Alibaba Group. Log Service supports collection, consumption, shipping, search, and analysis of logs, and improves the capacity of processing and analysing large amounts of logs. Log Service is a cloud-native observability and analytics platform that provides large-scale, low-cost, and real-time services to process multiple types of data such as logs, metrics, and traces. Log Service allows you to collect, transform, query, analyse, visualize, ship, and consume data. You can also configure alert rules in the console. Log Service helps you improve digital capabilities in R&D, O&M, and data security.
Type of Product	O&M and Monitoring
Key Features	• Fully-managed Service • Integrations and Configurations • Real-time Response • Comprehensive APIs and SDKs
Product Link	https://www.alibabacloud.com/product/log-service

6.5 Key Management Service (KMS)

(a) Areas of compliance:

- ✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	Easily protect, manage, use, and audit your cryptographic keys on Alibaba Cloud Alibaba Cloud KMS provides secure and compliant key management and cryptography services to help you encrypt and protect sensitive data assets. KMS is integrated with a wide range of Alibaba Cloud services to allow you to encrypt data across the cloud and to control its distributed environment. KMS provides key usage logs via ActionTrail, supports custom key rotation, and provides HSMs that have passed FIPS 140-2 Level 3 or other relevant validation, to help you meet your regulatory and compliance needs
Type of Product	Data Security
Key Features	• Comprehensive Management Features • Fully Managed HSMs • Integration with Other Alibaba Cloud Services • Simple and Effective Cryptographic Operations
Product Link	https://www.alibabacloud.com/product/kms

6.6 Web Application Firewall (WAF)

(a) Areas of compliance:

✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	Protects your websites and web servers based on the intelligent computing capabilities of Alibaba Cloud Security WAF provides end-to-end security protection for your websites or apps. WAF identifies, scrubs, and filters out malicious web traffic, and then forwards normal traffic to your origin servers. This protects your origin servers against attacks and ensures data and service security.
Type of Product	Cloud Security
Key Features	• Web Intrusion Prevention • Traffic Control and Bot Management • Data Security Protection • Security O&M and Compliance
Product Link	https://www.alibabacloud.com/product/web-application-firewall

6.7 Security Centre

(a) Areas of compliance:

✓ **Data Security - Privacy and Security Measures**

✓ **Data Security - Personal Data Breach Notification**

(b) Product Information

Topic	Description
Product Description	A unified security management system that identifies, analyses, and notifies you of security threats in real time. Powered by big data technologies, Security Centre provides protection from ransomware, various viruses, and web tampering. Security Centre also provides compliance assessment to protect cloud and on-premises servers and meet regulatory compliance requirements. Security Centre is fully compatible with third-party service providers. This reduces operations and maintenance (O&M) costs for security management.
Type of Product	Cloud Security
Key Features	• Security Protection • Proactive Defence • Threat Detection • Investigation and Response
Product Link	https://www.alibabacloud.com/product/security-center

6.8 Anti-DDoS

(a) Areas of compliance:

✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	A comprehensive DDoS protection for enterprise to intelligently defend sophisticated DDoS attacks, reduce business loss risks, and mitigate potential security threats. Anti-DDoS service is based on Alibaba Cloud's global scrubbing centres, combined with intelligent DDoS detection and protection systems developed at Alibaba, automatically mitigates attacks and reinforce the security of your applications, reduce the threat of malicious attacks.
Type of Product	Cloud Security
Key Features	• Global DDoS Protection Network for Volumetric Attack Mitigation • Intelligent Protection against sophisticated attack
Product Link	https://www.alibabacloud.com/product/ddos

6.9 Virtual Private Cloud (VPC)

(a) Areas of compliance:

✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	A virtual private cloud service that provides an isolated cloud network to operate resources in a secure environment. VPC helps you build an isolated network environment based on Alibaba Cloud including customizing the IP address range, network segment, route table, and gateway. In addition, you can connect VPC and a traditional IDC through a leased line, VPN, or GRE to provide hybrid cloud services.
Type of Product	Cloud Network
Key Features	• Layer-2 logical isolation • Custom network environment • Access control • Internet portal management • Hybrid cloud architecture
Product Link	https://www.alibabacloud.com/product/vpc

6.10 VPN Gateway

(a) Areas of compliance:

✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	VPN Gateway is an Internet-based service that establishes a connection between a VPC and your on-premise data centre. VPN Gateway is used to transmit encrypted traffic between Alibaba Cloud VPCs and enterprise data centres, enterprise office networks, or Internet platforms over the Internet. You can use this service to establish reliable and secure connections for data transmission.
Type of Product	Cloud Network
Key Features	• On-premise to cloud connections • Pay-As-You-Go and efficient management • Secure Internet platform connections
Product Link	https://www.alibabacloud.com/product/vpn-gateway

6.11 Block Storage

(a) Areas of compliance:

✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	Block-level data storage attached to ECS instances to achieve high performance, low latency, and high reliability. Block Storage is a block-level data storage service attached to Elastic Compute Service (ECS) instances and features low latency, persistence, and high reliability. Block Storage enables automatic replication within the same zone to avoid data loss caused by hardware failures and guarantee the stability and continuity of your workloads. You can manage Block Storage as you manage disks. For example, you can partition Block Storage devices that are attached to ECS instances and create file systems for Block Storage devices. You can also use Block Storage devices to achieve data persistence.
Type of Product	Storage Service
Key Features	• Online Scaling • Data Protection • Data Encryption • I/O Isolation
Product Link	https://www.alibabacloud.com/product/disk

6.12 Object Storage Service (OSS)

(a) Areas of compliance:

- ✓ **Processing of Personal Data - Retention**
- ✓ **Data Security - Privacy and Security Measures**

(b) Product Information

Topic	Description
Product Description	Fully managed object storage service to store and access any amount of data from anywhere. Alibaba Cloud OSS provides industry-leading scalability, durability and performance. Customers of all sizes and industries can use it to store and protect any amount of data for use cases, such as backup and restore, content distribution, data lakes, websites, mobile applications, data archive and IoT devices. OSS is designed for 99.999999999% (12 9's) durability, and backed up with industry-leading SLA. It helps millions of companies to build a scalable, secure and cost-effective storage foundation. It is also one of the key services that empowers Alibaba's Double Eleven event every year.
Type of Product	Storage Service
Key Features	• Bucket management • Object management • Access control • Data security • Data management • Log management • Data processing • Data lake management
Product Link	https://www.alibabacloud.com/product/object-storage-service

7. Alibaba Cloud Security & Privacy Protection Related Certifications

Alibaba Cloud is committed to protecting customers' personal information worldwide and complying with applicable laws of countries where our business operates.

In December 2018, Alibaba Cloud became the first cloud provider to attest to the additional requirements of the German C5: to demonstrate our commitment to a higher security standard. Furthermore, Alibaba Cloud is the first and currently only cloud provider in Singapore to attain all three key data protection certifications by the Infocomm Media Development Authority (IMDA) – the Data Protection Trustmark Certification (DPTM), the APEC Cross Border Privacy Rules (CBPR) System and Privacy Recognition for Processors (PRP) System.

Alibaba Cloud is a founding member of the EU Cloud Code of Conduct and the General Assembly, which is actively involved in the formulation of a code of conduct for EU cloud services following the requirements of the General Data Protection Regulation (“GDPR”) article 40, engages in constructive collaboration with the Data Protection department, and ensures that their expectations and future guidance for the GDPR are taken into account while drafting the code.

Alibaba Cloud is committed to maintaining a high standard of data protection throughout the Alibaba Cloud ecosystem and to contributing to the healthy development of the whole technology industry. In addition, Alibaba Cloud has demonstrated compliance with EU Cloud CoC by an independent review by SCOPE Europe.

Alibaba Cloud adopts industry standards and best practices to safeguard customer data. We have received multiple industry standard certifications and regularly complete third-party audits. Our compliance credentials include, but are not limited to:

Credentials	Description
ISO 27001	ISO27001 is a widely adopted global security standard that outlines the requirements for information security management systems. As the first cloud service provider to pass this certification in China, Alibaba Cloud proves that it has fulfilled security responsibilities in such aspects as data security, network security, communication security, and operational security.
ISO 27017	ISO 27017 provides a set of information security control guidelines for the use of cloud services, including additional implementation guidelines for ISO/IEC 27002-based controls, as well as additional controls and implementation guidelines related to cloud service features.
ISO 27018	ISO 27018 is an international standard for Personal Data protection that applies to cloud service providers. ISO 27018 provides a set of guidelines to protect personally identifiable information (PII) in public clouds. It is widely regarded as the strictest, most authoritative, and most widely accepted and applied information security system certification in the world.
CSA STAR	CSA STAR certification was developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI). Alibaba

	Cloud is the first company in the world to obtain the CSA STAR gold medal certification.
ISO 9001	ISO 9001 is an authoritative certification for quality management systems. It is designed to help organizations ensure that they meet the needs of customers and other stakeholders while meeting statutory and regulatory requirements related to a product or service.
ISO 20000	ISO 20000 is the first internationally recognized IT service management standard. As the first cloud service provider in China to obtain the ISO/IEC 20000-1:2011 certification, Alibaba Cloud has established and strictly implemented a standard service process. Standardized cloud services can improve efficiency and reduce overall risk.
ISO 22301	A standard for a Business Continuity Management (BCM) system, this certifies Alibaba Cloud as meeting the requirements for business continuity planning, disaster recovery, and regular drills to enhance the stability of the cloud platform.
ISO27701	ISO/IEC 27701:2019 is an extension of the ISO/IEC 27001 information security management system and ISO/IEC 27002 information security control measures. It has considered the mapping of GDPR clauses and other privacy-related standards from the very beginning and is an authoritative guideline for the construction of a privacy management system.
SOC1/2/3	Service Organization Control (SOC) reports are internal control reports on the services provided by a service organization. The reports provide valuable information that users need to assess and address the risks associated with an outsourced service.
Multi-Level Protection Scheme (MLPS) 2.0	Alibaba Cloud complies with the MLPS 2.0 standards in China. Alibaba Cloud's Finance Cloud is the first cloud platform that has passed the MLPS level-4 certification, and Alibaba Cloud's Government Cloud is the first cloud platform that has passed the MLPS 2.0 certification.
C5	Alibaba Cloud meets the C5 standard, showing its commitment to applying the highest level of compliance in control and security. The C5 standard serves not only as a benchmark for the German market, but also increasingly as a benchmark for institutions across Europe. With the attestation, German customers can leverage the work performed to comply with stringent local requirements and use Alibaba Cloud services to run secure workloads.
MTCS	The Multi-Tier Cloud Security (MTCS) Singapore Standard (SS584) is the world's first cloud security standard that covers multiple tiers of cloud security. MTCS has three levels of security, Level 1 being the base and Level 3 being the most stringent. Alibaba Cloud obtained the highest level of security: Level 3.
PCI DSS	The PCI Data Security Standards apply to all entities that store, process or transmit payment card information. Alibaba Cloud engaged with PCI SSC Approved Qualified Security Assessor (QSA) to conduct annual onsite assessment, i.e., PCI DSS v3.2.1 level 1 certified.
SEC Rule-17a	

Finra Rule 4511	Alibaba Cloud has completed the assessment related to the ability of OSS to comply with the broker-dealer media requirements promulgated by the Securities and Exchange Commission (SEC) Rule 17a-4(f) and Financial Industry Regulatory Authority (FINRA) Rule 4511. This assessment allows Alibaba Cloud to serve more customers in the financial industry worldwide, because these regulatory requirements have been widely adopted by many other countries outside of the US as part of the measurement of the financial support capability of a product.
TRUSTe Certified Privacy	Alibaba Cloud is certified by TRUSTe Enterprise Privacy & Data Governance Practices Certification program. This marks the compliance of Alibaba Cloud in collecting, using, managing, and destroying personal information.
HIPAA/HITECH	Alibaba Cloud fully supports the Business Associate Agreement (BAA) for customers that require strict compliance with the US Health Insurance Portability and Accountability Act (HIPAA) to protect the privacy and security of healthcare information. For detailed information, please refer to our HIPAA whitepaper, which covers compliance of multiple Alibaba Cloud products and services under HIPAA security requirements.
GxP	Alibaba Cloud has completed the GxP readiness assessment of our platform and products under the US Food and Drug Administration (FDA) Regulations on Electronic Records and Electronic Signatures (ERES) Part 11 of Title 21 Code of Federal Regulations (21 CFR Part 11).
TPN	As a “trusted partner” vendor, Alibaba Cloud is the first public cloud service provider to obtain the entertainment industry’s TPN (Trusted Partner Network) certification to ensure customers’ content security.
TISAX	Alibaba Cloud Germany passed the European automotive industry's TISAX (Trusted Information Security Assessment Exchange) certification with the highest level, level 3
Trusted Cloud Label	Alibaba Cloud is a member of Trusted Cloud promoted by German Federal Ministry of Economics and Energy, and has obtained their quality label of reliable cloud services.
EU Cloud Code of Conduct	As a founding member of the EU Cloud Code of Conduct and a member of the General Assembly, Alibaba Cloud is actively involved in formulating a code of conduct for EU cloud services in accordance with the requirements of GDPR article 40. Alibaba Cloud verified to be adherent to and compliant to the EU Cloud Code of Conduct by SCOPE Europe, the Code’s independent monitoring body. This verification underpins the GDPR-related measures implemented by Alibaba Cloud for customers.
DPTM	The Data Protection Trustmark (DPTM) Certification Framework was developed based on adopting and aligning it with Singapore’s personal data protection act and incorporating elements of international benchmarks and best practices. Alibaba Cloud is the first cloud provider in Singapore certified with the Data Protection Trustmark.

APEC CBPR/PRP	The APEC Cross Border Privacy Rules (CBPR) System and Privacy Recognition for Processors (PRP) System were developed by APEC economies to build consumer, business, and regulator trust in cross-border flows of personal data. By simplifying customers reviewing process on flow of information across borders, the CBPR and PRP certifications help Alibaba Cloud reduce compliance time and costs. Furthermore, the certifications mean solutions and services built on Alibaba Cloud infrastructure are similarly held to the high standards required.
Cyber (Advocate) certification	Trust mark The Cyber Trust mark developed by the Cyber Security Agency of Singapore (CSA), is targeted at larger or more digitalized organizations and helps organizations to communicate their investment in cybersecurity as a competitive edge and to build trust with their customers.

8. Conclusion and Summary

At Alibaba Cloud, we prioritize protecting the Personal Data of our customers globally. We adhere to relevant laws and regulations in the markets where we operate and have implemented various security measures to ensure the privacy of our customers' data. We strive for high standards and quality in our products and services and are committed to providing stable, reliable, secure, and compliant cloud computing infrastructure services.

In addition to the security measures, our approach also ensures that we provide our customers with the tools and features to help control how their Personal Data are processed. This means that you can dictate how our tools and features assist you under your terms while enjoying the comfort of our secure landscape. Moreover, we can assure you that the Personal Data provided will not be used for any other purposes beyond the delivery of Alibaba Cloud services.

This Whitepaper can be used by the customers to determine whether Alibaba Cloud products and services are in line with the requirements of the PDPA and the privacy standards to which the customers are adhering to. Please note that the information provided here is provided for informational purposes only and is not intended to be represented as legal advice.

As we work to consistently improve our customers' security, Alibaba Cloud's security policies and processes may change from time to time. You can access our latest security whitepaper and other publications which may be useful for you.

Useful Resources

[Alibaba Cloud Trust Centre](#): Explore Alibaba Cloud's commitment to security, privacy, and transparency. This resource provides insights into compliance certifications, data protection practices, and global privacy frameworks.

[Security Compliance FAQs](#): A comprehensive FAQ section addressing key questions about Alibaba Cloud's adherence to security standards, compliance certifications, and data protection measures.

[Alibaba Cloud Security Whitepaper](#): This whitepaper details Alibaba Cloud's robust security infrastructure, showcasing its technologies, best practices, and compliance frameworks to protect customer data and applications.

[Alibaba Cloud Product Catalogue](#): Discover Alibaba Cloud's extensive suite of products and solutions, ranging from cloud computing to AI, big data, and IoT, tailored to meet diverse business needs.

References

Statutory Legislations & Amendments

[Personal Data Protection Act 2010 \[Act 709\]](#)

[Personal Data Protection \(Amendment\) Act 2024 \[Act A1727\]](#)

Regulatory Guidelines

[Personal Data Protection Guidelines on Data Breach Notification \(DBN Guidelines\)](#)

[Personal Data Protection Guidelines on the Appointment of Data Protection Officer \(DPO Guidelines\)](#)

[Personal Data Protection Guidelines No. 03/2025 on Cross-Border Personal Data Transfer \(CBPDT Guidelines\)](#)

[Guidance on the Preparation of Personal Data Protection Notices](#)



Established in 2009, Alibaba Cloud (alibabacloud.com), the digital technology and intelligence backbone of Alibaba Group, is among the world's top three IaaS providers, according to Gartner. It is also the largest provider of public cloud services in China, according to IDC. Alibaba Cloud provides a comprehensive suite of cloud computing services to businesses worldwide, including merchants doing business on Alibaba Group marketplaces, start-ups, corporations and public services.

Alibaba Cloud is the official Cloud Services Partner of the International Olympic Committee.

www.alibabacloud.com/contact-sales

