

Annex II: Technical and Organizational Measures [M1 (C2C), M2 (C2P) and M3 (P2P)]		
TRANSFER SECURITY MEASURES	GENERAL DESCRIPTION	Alibaba Cloud Measures
Measures of pseudonymisation and encryption of personal data	Pseudonymization - Measures that enable one to process 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, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures.	<p>Some capabilities such as tenant isolation are enabled by default, while other capabilities such as data encryption must be enabled and properly configured by customers to function properly.</p> <p>Customers can also use the native encryption capabilities of Alibaba Cloud products or Alibaba Cloud Data Encryption Service for security-sensitive data encryption, and use the managed Hardware Security Module (HSM) feature integrated with Key Management Service (KMS) for encryption key management.</p> <p>Alibaba Cloud Data Security Center provides nearly 30 built-in masking algorithms in six categories including hash, encryption, masking, replacement, shuffling, and transformation, and supports user-defined masking algorithms or parameters. Data Security Center ensures that data is masked without changing the original data distribution and the corresponding business system logic, and ensures the validity and availability of the data. Users can protect their data while accomplishing business needs at a low cost and high efficiency.</p>
	Encryption - Measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.	<p><u>End-to-end encryption</u> Alibaba Cloud uses end-to-end encryption to ensure data security, including encryption in transit, encryption at rest, and hardware-based encrypted computing service using Intel® Software Guard Extensions (Intel® SGX). Alibaba Cloud also provides HSM-based Data Encryption Service and SSL Certificates Service as part of a complete set of data encryption solutions.</p> <p><u>Encryption in transit</u> Cloud products use the SSL/TLS protocol to ensure data transmission security while users read and upload data. The Alibaba Cloud console uses HTTPS encryption for data transmission. Alibaba Cloud products provide API access points that have HTTPS encryption enabled with 256-bit key length to address the need for encrypted transmission of sensitive data.</p> <p><u>Encryption at rest</u> Alibaba Cloud allows users to encrypt data stored at rest in Alibaba Cloud services with integration of Alibaba Cloud Key Management Service (KMS). Alibaba Cloud supports the Advanced Encryption Standard with 256-bit key length ((AES256) for encrypting sensitive data at rest.</p>
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Confidentiality - Measures ensuring that information is accessed only by an authorized person and prevent the intrusion by unauthorised persons into systems and applications used for the processing of personal data.	<p><u>Access Management</u> Alibaba Cloud has policies and procedures established for logical access management of employee access rights. Access is granted with role-based access controls (RBAC) and following the rule of the least privileges necessary for the operations platform. Only authorised personnel can access to IT infrastructure, which includes operating systems, database management systems and network devices. Root accounts are intended for direct login and password to root accounts is automatically rotated on a monthly basis via a scheduled job. Root privileges are restricted to authorised personnel only and privileged sudo to root activities are logged and monitored by the central log management system. Alibaba Cloud enforces two-factor authentication to authenticate users of the operations platform.</p> <p><u>Password Policy</u> Alibaba Cloud uses an identity authentication system for centralised authentication to the systems and resources within the Alibaba Cloud's environment, with Single Sign-on enabled. Password policies have been established and implemented, which require users to set up a password that meets the password requirements including password length, password complexity, password age, password history, maximum login attempts, and change of initial password.</p> <p><u>Environment Segregation</u> Alibaba Cloud maintains separate production, testing and development environments. Access to these environments are restricted to the authorized personnel. Controls are in place to ensure segregation of duties.</p> <p><u>Remote Access Management</u> To access Alibaba Cloud's intranet through VPN from the internet, employees must pass two-factor authentication based on domain account name and password plus dynamic digital token received on registered devices. Data Leakage Prevention ("DLP") software is installed on employees' registered devices to detect sensitive operations performed on the devices.</p> <p><u>Security and Privacy Training</u> Alibaba Cloud has established a training program for the needs of employees and management. The applicable policies, standards and information security and privacy practices are covered under training module. The information security and privacy training is provided to employees on an ongoing basis. As part of the training process, employees must pass data security test after completion of security awareness training.</p>
	Integrity - Measures ensuring that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.	<p><u>Network Security</u> Alibaba Cloud's applications and network are protected by WAF. A network intrusion detection system is utilized to monitor network traffic and user operations in real-time, and identify abnormal activities. The security team will follow up on the abnormal activities identified and take necessary actions.</p> <p><u>Log Monitoring</u> Alibaba Cloud collects logs from underlying infrastructure and system components. Logs are processed and analysed using pre-defined threat detection models for anomaly analysis and detection. The security team reviews the anomalies identified to verify whether any of them are security incidents or not. Security incidents discovered are then escalated to the corresponding teams for timely remediation.</p>
	Availability and resilience - Measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences, and ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.	Alibaba Cloud employs distributed storage. Files are split into multiple data segments and stored on different devices. Each data segment is stored in multiple replicas. Distributed storage improves data reliability and security. Based on product types/tiers and business needs, Alibaba Cloud products also provide multiple protection capabilities such as multi-copy redundancy, system backup, live migration, load balancing, and anti-DDoS to ensure high data availability. Multiple products offer backup capabilities that customer can choose to utilize.
Measures for ensuring the ability to restore the availability and access to personal Data in a timely manner in the event of a physical or technical incident	Measures that ensure the possibility to quickly restore the system or data in the event of a physical or technical incident.	<p>Alibaba Cloud has established business continuity plans. The business continuity management team performs business impact analysis and risk assessment, reviews and updates business continuity plans, as well as conducts Disaster Recovery drills every year.</p> <p>The business impact analysis and risk assessment include identification of critical business processes, maximum tolerable downtime, recovery time objective, minimum service levels and time needed to resume service. Threats that may trigger disruptions to Alibaba Cloud's business and resources are identified and documented, and corresponding strategies are designed according to different scenarios of cloud products and services. A business continuity drill covers data backup and recovery testing procedures and is updated when there are changes to products, services and the organizational environment.</p>

Annex II: Technical and Organizational Measures [M1 (C2C), M2 (C2P) and M3 (P2P)]		
TRANSFER SECURITY MEASURES	GENERAL DESCRIPTION	Alibaba Cloud Measures
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Measures that ensure the regular review and assessment of security measures.	<p>Alibaba Cloud carries out comprehensive assessment of information security management on an annual basis, including a review of information security policies, standards and requirements. Our legal and compliance departments monitor the legal, statutory and regulatory compliance obligations to ensure the company is aware of applicable compliance requirements in a timely manner. Our certifications include, but are not limited to:</p> <ul style="list-style-type: none"> •ISO 9001 Quality Management System •ISO/IEC 20000 Information Technology Service Management System •ISO/IEC 27001 Information Security Management System •ISO/IEC 27017 Code of Practice for Cloud-specific Information Security Controls •ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud •ISO 22301 Business Continuity Management System •ISO/IEC 27701 Privacy Information Management •Cloud Security Alliance's Security Trust and Assurance Registry ("CSA STAR") •Singapore Multi-Tier Cloud Security (MTCS) standard Level 3 •Payment Card Industry Data Security Standard (PCI-DSS) •Payment Card Industry Three-Domain Secure (PCI 3DS) •Service Organization Control (SOC) Reports 1/2/3 •German C5 standard Audit with Additional Requirements, type 2 •German Trusted Cloud Label •EU Cloud Code of Conduct under the GDPR •APEC Cross-Border Privacy Rules (CBPR) •APEC Privacy Recognition for Processors (PRP) •Singapore Data Protection Trustmark (DPTM) •Singapore Cyber Trust Mark <p>A detail list of regular assessments can be found at https://www.alibabacloud.com/trust-center/compliance</p>
Measures for user identification and authorisation	Measures to validate and authenticate users.	<p>Alibaba Cloud employees need to be authenticated through two-factor authentication ("2FA") based on registered devices and dynamic digital tokens to access Alibaba Cloud's office network from the internet. Employees need to be authenticated through 2FA based on password and dynamic digital token, to access to the production network from office network. Only authorised personnel can access to IT infrastructure, following the principle of least privilege and segregation of duties set forth in the Access Control Management Policy, to protect information assets from unauthorised access.</p> <p>Audit and monitoring rules have been defined within the access monitoring system to analyse usage of the accounts and access permission, detect potential misuse of access privileges, and generate automated alerts to notify security team of any deviations or exceptions.</p>
Measures for the protection of Data during transmission	Measures ensuring transmission control to ensure that personal data cannot be read, copied, changed or deleted without authorization during their transfer and that it can be monitored and determined to which recipients a transfer of data is intended.	<p>Alibaba Cloud uses high-security encryption algorithms such as AES256 and cryptographic protocols such as Ipsec and TLS in combination with strict authentication and authorization mechanisms to prevent encrypted data from being cracked. When customers perform operations by using the Alibaba Cloud Management Console, the console uses the HTTPS protocol for encrypted data transmission. All Alibaba Cloud services provide endpoints for access based on HTTP requests and supports transmission encryption by using a key up to 256 bits in length. This satisfies the requirements for encrypted transmission of sensitive data. Alibaba Cloud products such as VPN Gateway and Smart Access Gateway (SAG) provide secure transmission tunnels for customers to use. Additionally, Alibaba Cloud provides the capabilities for the customer to adopt TLS1.2 or above to ensure higher level of data security.</p>
Measures for the protection of Data during storage	Measures ensuring transmission control to ensure that personal data cannot be read, copied, changed or deleted without authorization while stored on data media.	<p>Alibaba Cloud isolates production networks from non-production networks. Direct access from a non-production network to any servers and network devices in a production network is not allowed. Alibaba Cloud isolates the cloud service network that provides services to external users from the physical networks that supports the underlying cloud service functionalities. Network ACLs are configured to prohibit access from cloud service network to physical network. Alibaba Cloud also takes network control measures to prevent unauthorized devices from connecting to the internal network of the cloud platform and prevent the physical servers of the cloud platform from initiating external connections.</p>
Measures for ensuring physical security of locations at which personal Data are processed	Measures for entry control, especially regarding legitimation of authorized persons	<p><u>Data Center Access Control</u></p> <p>At each Alibaba Cloud data center, long-term access permissions are assigned only to corresponding maintenance personnel. If it is necessary for any other person to enter the data center, the person must submit a formal application in advance, and is granted temporary permission only upon the approval of the corresponding department heads. For each entry to or exit from the data center, such persons must display their ID to check in, and be escorted by the data center's maintenance personnel for the entire duration of the visit.</p> <p>An Alibaba Cloud data center consists of equipment rooms, electrical measurement areas, warehouses, and other areas, with each area equipped with an independent access control system. Two-factor authentication (such as biometric verification) is employed for sensitive areas, and special areas are physically isolated by metal cages. All Alibaba Cloud data centers and office areas have access control, with visitor areas marked out separately. Visitors are required to carry entry pass and be escorted by Alibaba Cloud staff when visiting Alibaba Cloud premises. Data center managers perform a monthly review of the access card system and fingerprint access control system to ensure that only authorized personnel are granted access.</p> <p><u>Data Center Physical Security</u></p> <p>Smoke detectors, lightning protection and grounding devices, fire alarms and spray system, power supply system, shunting circuit system and control panel, fresh air system and air conditioning system are installed in data centers. The data center service providers are responsible for monitoring the smoke detectors, lightning protection and grounding devices, fire alarms and spray system, power supply system, shunting circuit system and control panel, fresh air system and air conditioning system, etc. In addition, maintenance personnel take shift work at data centers, to ensure 24/7 resolution of equipment malfunctions. The data center service providers have installed video surveillance at the entrance of data centers, equipment delivery areas and other sensitive areas. Personnel on duty at the monitoring rooms monitor the operation of the data centers 24/7.</p> <p>Alibaba Cloud performs monitoring on the server performance of the data center. A temperature monitoring system is in place to monitor the temperature of data center servers. If any exception occurs, an alert will be triggered automatically by the system. An equipment monitoring system is utilized to monitor the performance of servers. In case of a server performance exception, an alert is automatically triggered, and on-site operators follow up to resolve the issue.</p>

Annex II: Technical and Organizational Measures [M1 (C2C), M2 (C2P) and M3 (P2P)]		
TRANSFER SECURITY MEASURES	GENERAL DESCRIPTION	Alibaba Cloud Measures
Measures for ensuring events logging	Measures for ensuring the verifiability of event log files	<p>A log management platform is utilized to separately record user operations in the operating systems of products, as well as operating systems, database management systems and network devices supporting operation systems of products. The log files are protected from unauthorised access, modification and deletion. Audit and monitoring rules are defined within the log management platform to monitor sensitive activities and detect irregular user activities. The platform automatically generates alerts on irregular user activities for security team to review and follow up.</p> <p>In addition, Alibaba Cloud collects logs from underlying infrastructure and system components. Logs are processed and analysed using pre-defined threat detection models for anomaly analysis and detection. The security team reviews the anomalies identified to verify whether any of them are security incidents or not. Security incidents discovered are then escalated to the corresponding teams for timely remediation.</p>
Measures for ensuring system configuration, including default configuration	Measures to ensure that all in-scope systems and devices are compliant with baseline configuration settings	<p><u>Configuration Baseline</u></p> <p>Alibaba Cloud has established configuration baseline standards which specify standard configuration requirements for operating systems, database management systems, network devices, and virtual images with reference to CIS benchmark. The configuration baseline standards are reviewed and updated at least once a year. A configuration scanning tool is implemented to scan the configuration of operating systems, database management systems, network devices, and virtual images. The scanning results are analyzed and deviations from standard configurations defined in the baseline documents are detected and resolved by operation personnel. Alibaba Cloud's best practices for the secure configuration guidelines can be found at CIS Benchmark community site (https://www.cisecurity.org/benchmark/alibaba_cloud/)</p> <p><u>Change Management</u></p> <p>Alibaba Cloud has a formal change management procedure in place to govern the change made to the products and supporting infrastructure. Changes have to be approved before development. Proper testing and code review needs to be completed before deployment.</p> <p>Alibaba Cloud has implemented a SDLC solution tailored for cloud products to integrate security into each stage of the product development lifecycle in order to help improve the security capabilities and reduce the security risks of cloud products. To ensure that the products meet the rigorous requirements for cloud computing, a complete security development mechanism is put into place at six different stages, from product initiation, security architecture review, security development, security validation, product release, to incident response.</p>
Measures for internal IT and IT security governance and management	/	<p>Alibaba Cloud has established an Information Security Management System (ISMS) and certified the ISMS according to ISO/IEC27001:2013. Alibaba Cloud has also established IT Service Management System (ITSM) policies which are based on ISO/IEC20000-1:2011 and Business Continuity Management Systems in accordance with ISO/IEC22301:2012. On a yearly basis, Alibaba Cloud performs a management review and documents the review results.</p> <p>Alibaba Cloud has established a risk management framework to identify, analyze and manage risks within the company and those related to services provided. The risk management framework involves management and various teams, and covers strategic and operational risks. Our comprehensive risk management system is created in accordance with the ISO27001:2013 Standard, which requires an information security risk assessment to be carried out periodically. In addition, a risk rating for changes based on potential impact and likelihood of occurrence is also performed to ensure more additional resources and control measures are dedicated to higher risks. We also update our security policies according to the assessment results based on the result of information security risk assessment.</p>
Measures for certification/assurance of Processes and products	Certifications	<p>Alibaba Cloud carries out comprehensive assessment of information security management on an annual basis, including a review of information security policies, standards and requirements. Our legal and compliance departments monitor the legal, statutory and regulatory compliance obligations to ensure the company is aware of applicable compliance requirements in a timely manner. Our certifications include, but are not limited to:</p> <ul style="list-style-type: none"> •ISO 9001 Quality Management System •ISO/IEC 20000 Information Technology Service Management System •ISO/IEC 27001 Information Security Management System •ISO/IEC 27017 Code of Practice for Cloud-specific Information Security Controls •ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud •ISO 22301 Business Continuity Management System •ISO/IEC 27701 Privacy Information Management •Cloud Security Alliance's Security Trust and Assurance Registry ("CSA STAR") •Singapore Multi-Tier Cloud Security (MTCS) standard Level 3 •Payment Card Industry Data Security Standard (PCI-DSS) •Payment Card Industry Three-Domain Secure (PCI 3DS) •Service Organization Control (SOC) Reports 1/2/3 •German C5 standard Audit with Additional Requirements, type 2 •German Trusted Cloud Label •EU Cloud Code of Conduct under the GDPR •APEC Cross-Border Privacy Rules (CBPR) •APEC Privacy Recognition for Processors (PRP) •Singapore Data Protection Trustmark (DPTM) •Singapore Cyber Trust Mark <p>A detail list of regular assessments can be found at https://www.alibabacloud.com/trust-center/compliance</p>
Measures for ensuring Data minimisation	Measures to reduce the amount of data collected	<p>Alibaba Cloud strictly follows data minimisation principle when collecting personal information from our customers or end users. All of our new processes or products will go through a data protection impact assessment to ensure only necessary personal data are collected and processed for the purposes declared in the privacy policy (https://www.alibabacloud.com/help/en/legal/latest/alibaba-cloud-international-website-privacy-policy).</p> <p>Alibaba Cloud has implemented security measures to protect personal data throughout its lifecycle, including strong encryption requirements, strict access and authorisation policies, data retention policies, secure destruction requirements, etc. Alibaba Cloud has established internal supervision mechanisms to ensure that the data security requirements, including the preceding security measures, are strictly enforced.</p>

Annex II: Technical and Organizational Measures [M1 (C2C), M2 (C2P) and M3 (P2P)]		
TRANSFER SECURITY MEASURES	GENERAL DESCRIPTION	Alibaba Cloud Measures
Measures for ensuring Data quality	Measures to ensure that the data pipeline creates and sustains good data quality	<p>Customers can change, update or delete their registration data via Alibaba Cloud international management console on their own. Alibaba Cloud will then follow their instructions to change, update or delete their data.</p> <p>Alibaba Cloud has implemented security measures to protect personal data throughout its lifecycle, including strong encryption requirements, strict access and authorisation policies, data retention policies, secure destruction requirements, etc. Alibaba Cloud has established internal supervision mechanisms to ensure that the data security requirements, including the preceding security measures, are strictly enforced.</p>
Measures for ensuring limited data retention	Data retention	<p>Alibaba Cloud has established data retention and secure destruction policies. In general, personal data will not be kept beyond the period necessary for the purposes of data processing. Personal data should be sanitised and securely deleted upon the end of retention period.</p> <p>Customers can manage, delete, and perform other operations on their business data. Alibaba Cloud cannot access to or delete customer's data without their authorisation. Customers can set retention period of the business data while using Alibaba Cloud products and services according to their specific needs. For example, Object Storage Services (OSS) provides capabilities for customers to configure time-based retention policies for buckets. It also supports the Write Once Read Many (WORM) strategy that prevents an object from being deleted or overwritten within a specified period of time.</p> <p>After a customer releases a service or deletes data, Alibaba Cloud will delete the same as per the customer's instructions. Alibaba Cloud also provides an account deletion function, which achieves systematic account deletion. The data erasure technology of Alibaba Cloud meets industry standards. Erasure operations are recorded for verification.</p> <ul style="list-style-type: none"> Delete data on hardware storage medium: If the hardware storage medium needs to be reused, Alibaba Cloud clears the data on the medium for multiple times to ensure that the data is completely erased and cannot be restored by forensics tools. Perform physical destruction: If the storage medium is no longer needed, Alibaba Cloud performs physical destruction on the medium. All data destruction or physical destruction processes can be traced back to records that point to one specific hardware device, such as data destruction logs or a surveillance video that records a physical destruction process. These records can be used as audit evidence.
Measures for ensuring accountability	Businesses must maintain certain records of the personal data that they process	Privacy by Design promotes privacy and data protection from the beginning. All of our newly released Alibaba Cloud products have been through a security review and a data protection impact assessment to ensure security and privacy considerations are embedded in the product.
Measures for allowing Data portability and ensuring erasure	/	<p>Alibaba Cloud has established processes for customers to request portability of their data or deletion of their data by contacting us at intlcompliance@service.aliyun.com or submitting a system ticket. Alibaba Cloud follows internal policies and procedures to handle customer request and respond to their request within a reasonable timeframe. In cases where Alibaba Cloud acts as a processor, we have no direct relationship with the individuals whose personal data we process. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct their query to Alibaba Cloud's client (the data controller). Our Data Protection Addendum to Alibaba Cloud International Website Membership Agreement (https://www.alibabacloud.com/help/en/doc-detail/42427.html) describing how do we serve our customers as a data processor.</p> <p>Customers can delete, modify, and perform other operations on their business data. Customers can export their data including log entries, files, custom images, database tables, and other business data from the cloud products and services they are using before releasing a service. After a customer releases a service or deletes data, Alibaba Cloud will delete the same as per the customer's instructions. After the customer's business data is deleted, the business data cannot be recovered, and the customer shall bear the consequences and responsibilities arising from the deletion. Alibaba Cloud is not obligated to retain, export, or return the customer's business data.</p>
Applied restrictions or safeguards for sensitive data (if applicable)	/	Alibaba Cloud does not collect or process special category data.