WSO2 Public Cloud

The WSO2 public cloud includes the following elements:

Asgardeo

Asgardeo provides a SaaS-based identity and access management (IAM) solution for managing user identities.

Choreo

Choreo is a SaaS application development suite designed to accelerate the creation of digital experiences. Companies can build, deploy, monitor, and manage cloud-native applications to increase developer productivity and focus on innovation.

Choreo Control Plane (CP)

Organizations can use the Choreo control plane components to define, create, observe, and manage APIs, integrations, applications, and cloud-native workloads. These workloads can be deployed to the cloud data plane or private data plane.

Choreo Data Planes (DP)

The workloads of Choreo subscribers are deployed on data planes.

Choreo Cloud Data Plane (CDP)

The Choreo cloud data plane is the default data plane for Choreo. It is available in the US and EU regions and fully managed by WSO2.

Choreo Private Data Plane (PDP)

Choreo subscribers can deploy their workloads on a private data plane, which provides enhanced isolation and control over subscriber workloads. WSO2 can manage private data planes on either WSO2-owned or subscriber-owned Cloud Service Provider subscriptions such as Azure, AWS, GCP, Vultr, etc. Subscribers can choose between Standard and Premium PDP configurations, each providing different levels of security and management models tailored to meet isolation and security requirements. For more details, please refer to the **PDP Security** section.

WSO2 Billing and Subscription Portal

The billing and subscription portal allows cloud subscribers to choose their preferred subscription options and view their usage.

Payment gateway (Stripe)

WSO2 public clouds utilize Stripe, a PCI-DSS-certified payment gateway provider. Subscribers enter their payment and billing information directly on Stripe when they are subscribing to paid plans.

Support Portal (ServiceNow)

WSO2 subscribers can raise support tickets through ServiceNow, our ticketing system.

Data Classification

Classification	Description
Public	This classification pertains to information approved for public release by WSO2 management and any unclassified documents.
Internal	This classification applies to the information shared within the WSO2 group.
Confidential	This classification applies to information restricted to designated individuals or groups within WSO2, with circulation kept to a minimum.
Restricted	This information is classified as strictly confidential and restricted to designated individuals within WSO2. Any circulation requires management approval. This includes: - Information where disclosure is disallowed by law or regulation. - Information where secrecy is crucial for its intended purpose. - Information where unauthorized disclosure could have a significant negative impact on the organization and its stakeholders.

Asgardeo

Type of data	Classification	Stored at	Purpose
Organization Administrator profiles and related data	Restricted	US deployment	User management
End user profiles and associated data	Restricted	Regional deployments	User management
User roles/scopes	Restricted	Regional deployments	Privilege management
Secrets (keys/tokens/certificates)	Restricted	Key management services (Key vaults)	For integrations and to facilitate service
Log and event data - Asgardeo	Confidential	Regional deployments	To facilitate service

Choreo

Type of data	Classification	Stored at	Purpose
Organization Administrator profiles and related data	Restricted	Asgardeo US deployment or in External IDP, which the subscriber integrates.	User management
End user profiles and associated data	Restricted	Asgardeo regional deployments or in External IDP, which the subscriber integrates.	User management
User roles/scopes	Restricted	Choreo control plane	Privilege management
Secrets (keys/tokens/certificates)	Restricted	Key management services (Key vaults)	For integrations and to facilitate service
Choreo component data	Confidential	Choreo control plane	To facilitate service
Observability data	Confidential	Choreo data plane	To facilitate service
Log and event data - Choreo user applications	Confidential	Choreo data plane	To facilitate service
Log data (audit and CI/CD)	Confidential	Choreo control plane	To enable service and legitimate interest (audit logs)
Business data used by Choreo user applications	Confidential	On the cloud services and region selected by the subscriber	To facilitate application storage needs such as databases, caches, and message brokers.

WSO2 public cloud common services

Type of data	Classification	Stored at	Purpose
Billing information	Restricted	Stripe* / billing module	Billing
Credit card data	Restricted	Stripe*	Billing
Log data - audit and security	Confidential	US and EU regional cloud security subscription - Azure	Legitimate interest

Support cases	Confidential	ServiceNow*	To provide support

* Third-party service providers (sub-processors). See the sub-processor list here.

Data Protection

Data subject is someone who can be identified from personal data. The data subject's rights will be addressed in the relevant data protection laws and regulations, such as the right to be deleted, informed, data portability, and object data processing, and not to be subject to profiling and automated decision-making.

Data controller is the legal entity or person that decides the purposes and means of processing personal data. The Data controller must comply with respective data protection laws and regulations and comply with data subject requests.

Data processor is the legal entity or the person who processes personal data on behalf of the controller. The Data processor must comply with respective data protection laws and regulations and comply with data subject requests.

WSO2's Role in Protecting Data

WSO2 has a dual responsibility as a Data controller and Data processor, depending on the purpose for which the personal data is consumed.

As the Data controller, WSO2 will collect personal data from the users interacting with WSO2 public cloud platforms, which are limited to:

- Collecting data to perform legal compliance screening requirements.
- Collecting data required for user registration or signup process.
- Collecting data required for billing and subscription purposes.
- Collecting data to protect the platform from security threats.
- Collecting data to improve our services.

As the Data processor, WSO2 will process data provided to WSO2 by the subscriber (who shall be the Data controller). For example, the subscriber is the Data controller for users they invite to WSO2 public clouds, and data is uploaded to WSO2 public clouds by the subscriber and its users.

WSO2 is the data controller for the "Organization Administrator profiles and associated data." This is because WSO2 decides what data is needed for the creation of cloud user profiles to facilitate the service for the subscriber.

The subscriber is the data controller for the "End user profiles and associated data." WSO2 is the data processor, as WSO2 processes the data shared according to the subscriber's instructions.

In an event where a partner is developing a subscriber's business use cases using WSO2 clouds and has access to personally identifiable information (PII) while managing the implementation. In that case, the partner also becomes the data processor as they may have access to PIIs and could define the application behaviors. WSO2 becomes a sub-processor in this instance.

Both the data controller and the data processor need to have a Data Processing Agreement (DPA) in place. The DPA should include provisions for passing on DPA obligations to any subprocessors used by the data processor. Additionally, the data processor and any subprocessors should also have a DPA between them.

As a Data processor, **WSO2 will be responsible for:**

- Processing personal data in accordance with the Data controller´s instructions.
- Safeguarding and protecting the Data controller's data in accordance with all required technical and organizational measures and data protection laws currently in force.
- Ensuring Data subject requests (DSRs) are addressed.
- Providing information and all reasonable assistance related to data privacy and security requests from the Data controller.
- Ensuring that sub-processors adhere to all data protection requirements and standards.
- Ensuring that WSO2 has adopted appropriate safeguards and adequate levels of protection for cross-border data transfers.
- Notifying the Data controller if WSO2:
    - receives requests from the subscriber's administrators and developers exercising their GDPR rights.
    - receives requests from any supervisory authorities (unless prohibited by law).
    - receives requests from any law enforcement authorities.
    - becomes aware of a confirmed security breach.
    - changes to privacy policies, terms, security statements, data protection agreements, processors, or sub-processors.

Subscriber’s Role in Protecting Data

The subscriber, as the Data controller, will be responsible for,

- Complying with relevant data protection laws and regulations as applicable to the subscriber.
- As between WSO2 and the subscriber, the subscriber will always remain in control of the data added by the subscriber or its users to the platform.
- Ensure subscribers' integrations with third-party applications are secure and in accordance with data protection requirements.
- Adhering to relevant security best practices as per WSO2 product documentation.
- Inform WSO2 of any data subject requests from subscribers' administrators and developers so that WSO2 can support the subscriber in processing the request. The subscribers can submit a request form or contact the data protection officer at dpo@wso2.com.
- Informing WSO2 of any vulnerabilities or security issues related to the platform.
- Complying with WSO2 public cloud Terms of Use.

Data Residency

Where is the subscriber data stored?

- Asgardeo
    - Asgardeo organization administrator profiles and associated data would be stored in Asgardeo US deployment.
    - Asgardeo end user profiles and associated data would be stored in the region where the deployment is provisioned (US or EU).
- Choreo
    - Choreo uses Asgardeo as its default identity provider.
        - Hence, both user profiles and associated data would be stored in Asgardeo US deployment.
    - If a subscriber wants to use their existing external IDP, the administrator and end-user profiles and associated data will remain within that IDP.
    - Choreo's control plane stores specific component data in US deployment.
    - Choreo applications and associated data would reside in the region where the data plane would reside.
        - Choreo cloud data plane - US - Azure
        - Choreo cloud data plane - EU - Azure
        - Choreo private data plane - subscriber's preferred data center region (AWS, Azure, GCP, OnPrem)
- WSO2 public cloud's billing and support portals are hosted in the US.

Can subscribers govern where their data is hosted?

- Asgardeo
    - Asgardeo subscribers can select US or EU data centers to store user data while provisioning the Asgardeo organization. However, the Asgardeo organization administrator profile data would be residing in the Asgardeo US deployment. For more details, please refer to "Data residency in Asgardeo."
- Choreo
    - Choreo subscribers can host their workloads on the Choreo cloud data plane (US and EU) or private data planes in a region and a cloud or a data center of their preference. However, Choreo control plane data would reside in the US.
    - Choreo also simplifies creating databases, caches, and message brokers for user applications on GCP, AWS, Azure, and DigitalOcean, with deployment options in the US, EU, and Australia if they prefer to use application dependencies created through Choreo instead of connecting to their existing resources.

Is subscriber data transferred around the world?

WSO2 would not transfer data outside of the region where the data is residing. The WSO2 team would have limited access to deployment data; please refer to the Data Access section.

What is the legal basis for WSO2 cross-border data transfers?

WSO2 operates globally and may transfer, store, access, or process subscriber's personal data across its affiliates and authorized sub-processors to provide the purchased services.

For transfers of personal data originating from the EU, WSO2 relies on valid legal mechanisms, including adequacy decisions or the EU Standard Contractual Clauses (2021). WSO2 ensures that all cross-border data transfers from the EU comply with GDPR requirements.

WSO2 employees across WSO2 subsidiaries and affiliate companies access personal data collected by WSO2 solely to provide subscription and professional services for the subscriber. This includes ancillary operational activities related to subscription and professional services, such as account management and invoicing. Additionally, data collected from visitors to the WSO2 websites are accessed for website-related functionalities and services.

This data will be accessed exclusively by WSO2 employees and the authorized subprocessors involved in the activities mentioned above.

Data Access

Who has access to subscriber data?

- The Site Reliability Engineering (SRE) team would have access to the public cloud deployments to perform maintenance, administration, troubleshooting, and support. Only the SRE team is granted access to the deployments and their data. Other teams would need to go through service requests and change requests to gain deployment-related data access if required.
- The Customer Reliability Engineering (CRE) team, which would interact with subscribers to support queries and issues, would have access to subscriber information on our support ticketing system and log data.
- The security team would have access to log data to monitor and respond to security events and incidents.
- WSO2 account managers would have access to the support ticketing system and CRM for account management.

How do WSO2 employees access the cloud infrastructure?

WSO2 uses Azure Privileged Identity Management (PIM) to control access to Azure resources. SRE team members must activate their eligible roles and submit requests for access. The team consists of specialized sub-teams, like Asgardeo-SRE and Choreo-SRE, ensuring no shared access across deployments. WSO2 also employs VPN connections with one-time passwords (OTPs) and uses Bastion instances for administrative tasks.

From what locations do you access data?

Following are the locations where our teams are residing,

- SRE - Sri Lanka, India, Brazil.
- CRE - Sri Lanka, India, Australia, Brazil, Spain, UK, USA.
- Security - Sri Lanka.
- Account Management - Sri Lanka, USA, UK, Germany, Spain, Australia, India, Brazil, Dubai, and Singapore.

Technical and Organizational Controls

Cloud Security

Please refer to our cloud security process for detailed information on incorporating security into public clouds.

PDP Security

We offer Standard and Premium Private Data Planes (PDPs), each designed with varying levels of security to balance cost and protection. If you are interested in using a PDP, please ensure you select the appropriate tier and add-ons that meet your specific requirements. For detailed information, please refer to the documentation on Private Data Plane Security Levels and Private Data Plane Management Models.

Data Encryption

What options are available for subscribers to encrypt their data?
Choreo provides robust encryption mechanisms for system components in the data planes, leveraging cloud service provider (CSP) and cloud-native technologies to ensure the security of subscriber's data. This built-in encryption offers seamless protection for system-level components.

Additionally, application developers have the flexibility to implement their own encryption mechanisms to safeguard their business data. This allows developers to tailor security solutions to meet specific organizational or regulatory requirements, ensuring maximum control over data protection strategies.

How is data encrypted in transit?
WSO2 encrypts data in transit by leveraging TLS 1.2. Furthermore, all CDP and PDP communications within the cluster are encrypted using Cilium WireGuard encryption. WireGuard uses the ChaCha20 encryption algorithm with a 256-bit key.

How is data encrypted at rest?
WSO2 ensures data at rest is encrypted using cloud service provider (CSP) technologies, including disk and database encryption. These mechanisms typically utilize AES-256 encryption to provide robust security.

How are Secrets encrypted?
Secrets are encrypted using cloud service provider (CSP) managed keys and securely stored in key management services, such as Key Vaults. These services ensure robust encryption, centralized management, and controlled access to sensitive data.

Are application service users stored securely?
Choreo ensures that application service users are stored and managed securely by leveraging trusted and industry-standard identity providers.

- **User Authentication**: Choreo primarily authenticates users through well-established social logins, such as Google, GitHub, and Microsoft, ensuring the security of user credentials. Additionally, Choreo supports Enterprise ID logins, allowing seamless integration with your organization's identity provider for Single Sign-On (SSO). This means the complexity of password management is handled by the chosen identity provider, not Choreo itself, minimizing security risks.
- **API Consumer Authentication and Authorization**: Choreo uses Asgardeo as the default external identity provider (IDP), which can be used to securely manage end-user identities. If you prefer to use an external IDP like Azure Active Directory, Choreo allows flexible integration, ensuring that user management and authentication are securely handled by the respective external IDP.
- **User Tokens**: The Choreo Console stores the tokens in the browser's session storage and uses them to authenticate the user with the backend services. Choreo CLI persists the tokens in an encrypted file in the local machine's file system. The key to decrypt the tokens is stored in the system's Keychain. Choreo VSCode Extension uses the Choreo CLI to manage the tokens and invoke backend services.

By utilizing these secure, trusted identity providers and protocols, Choreo guarantees that user data is securely managed, reducing the risk of unauthorized access.

Data Isolation

Choreo's Data Plane system components operate independently, relying only on the Choreo Control Plane for control instructions and user workload configuration. Once user workloads receive traffic, the Control Plane connection is no longer required, ensuring that the data plane's core functions remain isolated and unaffected by external dependencies.

Within the Data Plane, workloads are organized into projects following a cell-based architecture. This structure allows subscribers to control the visibility of their endpoints, deciding whether they are exposed to the public, accessible to other projects, or kept private within the project. This level of control reinforces service isolation by clearly delineating which services interact and how they are exposed.

System Availability

Uptime SLAs, along with exclusions and Service Credit plans, are detailed in the Choreo Support Policy.

Data Backups

How is data backed up, and how often?

- Asgardeo:
    - Asgardeo utilizes geo-redundant databases
    - SQL database backups
        - Database backups are geo-redundant
        - Full backup - weekly
        - Differential backups - every 12-24 hours
        - Transaction log backups - every 10 minutes
    - Storage accounts - every 4 hours
- Choreo:
    - For System Services:
        - Choreo utilizes geo-redundant databases.
        - SQL database backups
            - Database backups are geo-redundant
            - Full backup - weekly
            - Differential backups - every 12-24 hours
            - Transaction log backups - every 5-10 minutes
        - MongoDB
            - Continuous, hourly, daily, weekly, monthly
        - Container registries and storage accounts are geo-redundant; Hence, they are not backed up separately.
        - OpenSearch performs daily backups of logs to AWS S3 Standard buckets, which are designed to be availability zone-redundant.
        - The Redis Cluster performs data backups every 6 hours and is stored in AWS S3, Vultr Object Storage (S3-compatible), and Azure Blob Storage, with plans to include Google Cloud Storage (GCS) in GCP.
    - For User Applications:
        - Choreo-Managed Postgres
            - Choreo runs full backups daily to automatically back up Choreo-managed PostgreSQL databases and copies the write-ahead logs (WAL) at 5-minute intervals or for every new file generated.
        - Choreo-Managed MySQL
            - Choreo runs full backups daily to automatically back up Choreo-managed MySQL databases and record binary logs continuously.
        - Choreo-Managed Cache
            - Choreo runs full backups daily to automatically backup Choreo-Managed Caches and has write-ahead logs (WAL) copied at 5-minute intervals or for every new file generated.

How long is backed-up data kept?

- Asgardeo:
  - SQL database backups - 1 month
  - Storage accounts - 1 month
- Choreo:
  - For System Services:
    - SQL database backups - 7 days
    - MongoDB backups
      - Hourly backups - 2 days
      - Daily backups - 7 days
      - Weekly backups - 4 weeks
      - Monthly backups - 13 months
    - OpenSearch
      - Daily backups - 1 year
    - Redis Cluster
      - Daily backups - 2 days
  - For User Applications:
    - Choreo-Managed Postgres and MySQL
      - The frequency of backups and retention varies according to plan: Hobbyist offers single disaster recovery backups, while Startup, Business, and Premium provide 2, 14, and 30 days of point-in-time recovery (PITR), respectively.
    - Choreo-Managed Cache
      - The frequency of backups and retentions varies by plan: Hobbyist offers a single disaster recovery backup, while Startup, Business, and Premium provide backups every 12 hours for up to 1, 3, and 13 days, respectively.

Are backups encrypted?

Backups are encrypted with CSP-managed keys.

Can subscribers restore data if they need to?

Soft delete is not supported, but where applicable, mandatory user confirmation is required before triggering the delete action. Backups and restorations are operational procedures that are not exposed to subscribers.

Logging and Monitoring

How long are logs available?

- Security logs are retained online for 90 days and archived for 1 year.
- Asgardeo logs are retained online for 30 days and archived for 1 year.
- Choreo logs are retained online for 30 days and archived for 1 year.

Are you monitoring the cloud platform?

Our security operations center (SOC) continuously monitors, detects, analyzes, and responds to cyber threats related to the Choreo Control Plane, Choreo Cloud Data Plane, and Asgardeo Deployments.

SOC monitoring is an add-on for Premium PDPs and Private Clouds; it does not monitor standard PDPs.

Incident Response

Would you notify subscribers in the event of a data breach or security incident?

In a security incident or data breach, if we discover that our subscribers are impacted, we would notify the affected subscribers immediately, not exceeding 48 hours.

Audits

Can subscribers perform penetration tests?
Yes, subscribers can perform penetration tests with prior approval for their paid subscriptions. Subscribers have to bear the cost incurred and follow data clean-up procedures. The penetration tests must ensure that any identified security vulnerabilities are informed and that data is not disclosed or disrupted by other subscribers (e.g., tests related to DDoS and DoS mitigation techniques).

What should subscribers do if they discover a vulnerability?
Subscribers can report security vulnerabilities or threats using the support portal or email channels listed on the Report Security Issues page.

Internal Audits
The WSO2 security and compliance team performs periodic internal audits on WSO2 public clouds based on predefined baseline standard checklists. These checklists are updated periodically to ensure they reflect the latest technological advancements. The reports of these audits are shared with senior management to identify and execute the necessary corrective actions.

Certification Audits
As part of WSO2's compliance initiatives, external parties who provide compliance certifications carry out annual audits on the WSO2 Public Cloud offerings (Asgardeo and Choreo). During these audits, the results of internal audits are also reviewed to ensure that periodic auditing is taking place.

Can subscribers audit WSO2 public clouds?
WSO2 does not permit its subscribers to perform their audits on public clouds as this is a SaaS-like service offering. However, under confidentiality agreements, we can share limited external audit reports on a case-by-case basis.

Compliance

Are WSO2 public clouds SOC 2 compliant?
WSO2 has successfully obtained the SOC 2® Type 2 report for Security, Confidentiality & Processing Integrity Trust Service Criteria with HITRUST CSF mapping for our Public Cloud service offerings, Asgardeo (US and EU deployments) & Choreo (Choreo Control Plane and Cloud Data Planes excluding Private Data Planes which needs to be certified separately upon subscriber's requirement). We intend to continue operating the control environment and plan to undergo SOC 2® audits annually.

Are WSO2 public clouds GDPR compliant?
WSO2 is compliant with the requirements of GDPR.

Are WSO2 public clouds CCPA compliant?
WSO2 is compliant with the requirements of CCPA.

Are WSO2 public clouds ISO/IEC 27001:2013 certified?
WSO2 public clouds are not ISO/IEC 27001:2013 certified. However, the WSO2 digital operations team manages WSO2's corporate infrastructure, and cloud access is ISO/IEC 27001:2013 certified. We completed the ISO Surveillance and Upgrade Audit in December 2024 and have been recommended for continuation and an upgrade to the ISO/IEC 27001:2022 version.

Are WSO2 public clouds PCI DSS certified?
Choreo Public Cloud offering (Control Plane and Cloud Data Plane) is certified by PCI DSS v4.0 Level 1.

Are WSO2 public clouds HIPAA compliant?
WSO2 public clouds are not HIPAA compliant. However, our SOC 2 report includes applicable HITRUST CSF control mapping.

Supplier Management

Do WSO2 public clouds use subcontractors?
WSO2 does not subcontract services related to WSO2 public clouds.

Do WSO2 public clouds use subprocessors?
WSO2 leverages subcontractors who provide us with specific services in our Public Cloud Subprocessor List.

Does WSO2 perform vendor security risk assessments (VSRAs)?
A team composed of IT, security, legal, HR, and finance would vet all suppliers, subcontractors, service providers, and vendors to ensure that external entities meet WSO2 standards. During the evaluation process, we would leverage vendors' security certifications, attestations, and security responses.

Termination of Subscription

Can subscribers request a backup or copy of the data?

- Asgardeo:
  - This can be facilitated via a support request for paid subscribers.
- Choreo:
  - No, subscribers can only request the PII stored in Choreo. No raw data backups are shared.

What is the data destruction process?

- Asgardeo:
  - Upon receiving a request for data destruction, it would take up to 30 days to complete.
- Choreo:
  - The data associated with the subscriber's organization would get wiped out within 4 months.

Contacting WSO2

How can subscribers communicate with WSO2?

- General queries can be raised at
    - Asgardeo:
        - Email: asgardeo-help@wso2.com
        - Discord: https://discord.com/invite/Xa5VubmThw, channel: #help-asgardeo
    - Choreo:
        - https://wso2.com/choreo/customer-support/
- Security issues or vulnerabilities can be raised at
        - https://wso2.com/security/
- Privacy concerns can be raised at
        - https://wso2.com/data-privacy-protection-request/

Revision History

Release Date	Summary of Changes
2023-02-22	Initial release
2023-10-17	Updates, - Asgardeo and Choreo EU deployments. - Asgardeo and Choreo data classifications. - Public cloud compliances.
2025-01-09	Updates - Backup and data retention frequencies - New public cloud sub-processor list - Compliance statement updates