WSO2 Public Cloud

WSO2 public clouds comprise the following components:

Asgardeo

Asgardeo is a SaaS-based customer identity and access management (CIAM) solution that integrates with Choreo. This is where the user identities would be managed.

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.

Control Plane

The Choreo Control Plane consists of many components that help developers to define, create, observe, and manage APIs, integrations, applications, and cloud native workloads. Developers can deploy their APIs, integrations, applications, and cloud native workloads to the Choreo Cloud Data Plane or their Private Data Plane.

Choreo Data Planes

Choreo Cloud Data Plane

The Choreo Cloud Data Plane is the default Data Plane available on Choreo. It is fully managed by WSO2 and runs on Microsoft Azure. It enables companies to create and launch apps in minutes and avoid concerns about the underlying infrastructure.

Choreo Private Data Plane

Choreo customers can deploy their workloads to their own private data plane. It can be operated alongside the user's current cloud services, such as Azure, AWS, GCP, or a Kubernetes cluster that runs on-premise.

WSO2 Billing and Subscription Portal

The billing and subscription portal allows public cloud subscribers to choose the required subscription options and see the usage.

Payment Gateway (Stripe)

Stripe is the PCI-DSS-certified payment gateway service provider used in WSO2 public clouds. When a customer chooses a subscription, the customer is prompted to enter their credit or debit card information and billing addresses on Stripe directly.

Support Portal (ServiceNow)

WSO2 uses ServiceNow as our support ticketing system, where WSO2 subscribers can raise support tickets via this platform.

Data Classification

Classification	Description
Public	This classification applies to information, which has been explicitly approved by WSO2 management for release to the public, and to any document which has not been classified under any other category.
Internal	This classification applies to information that can only be shared within the WSO2 group.
Confidential	This classification applies to information that is specifically restricted to a designated individual(s) or group in WSO2. Circulation is kept to a minimum.
Restricted	This classification applies to information that is specifically restricted to a designated individual(s) in WSO2. Circulation is strictly prohibited and requires management approval. This information would be - Information where disclosure is disallowed by law or regulation. - Information where the secrecy of it is crucial for its intended purpose. - Information where unauthorized disclosure could have a significant negative impact on the organization and its stakeholders.

Type of data	Classification	Stored at	Purpose
User Profile	Restricted	Asgardeo	User Management
User Credentials	Restricted	Asgardeo	User Management
User Roles/Scopes	Restricted	Asgardeo	User Management
Billing Information	Restricted	Stripe* / Billing Module	Billing
Credit Card Data	Restricted	Stripe*	Billing
Secrets (keys/tokens/certificates)	Restricted	Key Vaults (Azure/AWS*)	For Integrations and to facilitate service
API Management Data	Confidential	Choreo Control Plane	To facilitate service
Observability Data	Confidential	Choreo Control Plane	To facilitate service

Log and Event Data - Asgardeo	Confidential	Asgardeo	To facilitate service
Log and Event Data - Choreo	Confidential	Choreo Control Plane	To facilitate service
Log Data - Security	Confidential	Choreo Control Plane	Legitimate interest
Support Cases	Confidential	ServiceNow*	To provide support

* Third-party service providers (sub-processors). See the sub-processor list at WSO2 Subprocess List.

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, right to be informed, right to data portability, right to 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 in respect of users they invite to WSO2 public clouds and data uploaded to WSO2 public clouds by the Subscriber and its users.

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 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

Subscriber as the Data Controller will be responsible for

- Complying with relevant data protection laws and regulations as applicable to 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.
- Ensuring Subscriber´s 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.
- Informing WSO2 of any data subject requests from subscriber’s 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 customer data hosted?
WSO2 Public clouds are hosted in Microsoft Azure.

Where are the data centers located?

- *The following WSO2 Public Cloud components are located in the USA.*
  - *Asgardeo*
  - *Choreo Control Plane*
  - *Choreo Cloud Data Plane*
  - *WSO2 Cloud Billing*
  - *Support Portal*
- *Following WSO2 Public Cloud components can be hosted in a region based on customer preference.*
  - *Choreo Private Data Plane*
- *WSO2 is working on creating an EU deployment.*

Can customers govern where their data is hosted at?
When using the Private Data Plane in Choreo, Customers would have the ability to host the private data plane in a region and cloud of their preference and connect to the data sources and expose APIs through the private data plane.

Is customer data transferred around the world?
WSO2 Public Cloud would be hosted in the Azure US region by default. The DevOps team would primarily manage WSO2 Public Cloud deployments, and the Customer Success team would provide customer support services. These teams are based in Sri Lanka, Brazil, the US, and the UK.

What is the legal basis for WSO2 cross border data transfers?
WSO2 transfers data to its affiliate entities providing services globally. The basis for transfers originating from the EU is either an adequacy decision to an approved third country or the EU Model Standard Contractual Clauses issued in 2021. WSO2 ensures that all cross border data transfers originating from the EU are in accordance with GDPR requirements.

Technical and Organizational Controls

Cloud Platform Security

Please refer to our Securing WSO2 Private and Public Clouds document.

Data Encryption

What options are available for customers to encrypt their data?
We don't facilitate customers to encrypt their data. We use Azure Managed Services to encrypt customer data.

How is data encrypted in transit?
WSO2 uses end-to-end encryption. Minimum TLS 1.2 is enforced.

How is data encrypted at rest?
WSO2 utilizes Azure-managed services to encrypt data at rest.

How are Secrets encrypted?
Secrets are encrypted using Azure key vaults. WSO2 uses Azure-managed Keys.

Data Backups

How is data backed up, and how often?

- *Asgardeo:*
  - *SQL database backups*
    - *Full backup - Weekly*
    - *Differential backups - Every 12-24 hours*
    - *Transaction log backups - Every 10 minute*
  - *Storage accounts - Every 4 hours*
- *Choreo:*
  - *SQL database backups*
    - *Full backup - Weekly*
    - *Differential backups - Every 12-24 hours*
    - *Transaction log backups - Every 5-10 minute*
  - *NoSQL database backups*
    - *Continuous, Hourly, Daily, Weekly, Monthly*

How long is backed-up data kept?

- *Asgardeo:*
  - *SQL database backups - 1 month*
  - *Storage accounts - 1 month*
- *Choreo:*
  - *SQL database backups - 7 days*
  - *NoSQL database backups*
    - *Hourly backups - 2 days*
    - *Daily backups - 7 days*
    - *Weekly backups - 4 weeks*
    - *Monthly backups - 13 months*

Are backups encrypted?
Backups are encrypted with Azure Managed Keys.

Can customers restore data if they need to?

- *Soft delete is not supported, but mandatory user confirmation is taken before triggering delete action where applicable. The backups and restores are operational procedures and not exposed to the customers.*

Data Access

Who has access to customer data?

- *The DevOps team would have access to the Public Cloud Deployments to perform maintenance, administration, troubleshooting, and support.*
- *The Customer Success team, who would be interacting with customers to support customer queries and issues, would have access to customer 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 ticketing system and CRM (Customer Relationship Management).*

How do WSO2 employees access the cloud infrastructure?

WSO2 leverages Azure Identities and Privileged Identity Management (PIM) to grant access to Azure resources. The DevOps team member needs to activate the assigned eligible role by requesting to gain access to resources. In addition, WSO2 leverages VPN connectivities with OTP and Bastion instances to perform administrative tasks.

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 1 year.*
- *Choreo logs are retained online for 30 days and archived for 1 year.*

Are you monitoring the cloud platform?

WSO2 Security Operations Center (SOC) monitors the WSO2 public cloud environments.

Incident Response

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

In a security incident or data breach, if we discover our customers were impacted, we would notify the customers immediately, not exceeding 72 hours.

Audits

Can customers perform penetration tests?

Yes. Customers can perform penetration tests with prior approval on their paid subscriptions using external tools or services. Customers have to bear the cost incurred and follow data

clean-up procedures. The penetration tests must ensure that any security vulnerabilities identified are informed and do not disclose data and disrupt other customers (for example, tests related to DDoS and DoS mitigation techniques).

What should customers do if they discover a vulnerability?
Customers can use support and email channels listed at https://wso2.com/security/ to report security vulnerabilities.

Internal Audits
WSO2 Security and Compliance team performs quarterly internal audits 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 the Senior Management in order 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 environment. During these audits, the results of Internal Audits are also reviewed to ensure periodic auditing is taking place. The certification shall be granted/renewed only if WSO2 successfully completes the audit.

Can customers audit WSO2 Public Clouds?
WSO2 usually does not allow customers to perform their own audits on Public Clouds. However, on request, we can make arrangements to share limited external audit reports on a case-by-case basis.

Compliance

Are WSO2 Public Clouds SOC 2 compliant?
We are working on SOC 2 compliance (Security, Confidentiality & Processing Integrity Trust Service Criteria). The Type 1 report is expected by the end of Q1 2023.

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 FedRamp compliant?
WSO2 is currently evaluating the initiation of a FedRAMP compliance initiative.

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 who manages WSO2's corporate infrastructure is ISO/IEC 27001:2013 certified.

Are WSO2 Public Clouds PCI DSS certified?
WSO2 Public Clouds are not PCI-DSS compliant and included in WSO2's Compliance Roadmap.

Are WSO2 Public Clouds HIPAA compliant?
WSO2 Public Clouds are not HIPAA compliant.

Supplier Management

Do WSO2 Public Clouds use subcontractors?
WSO2 does not subcontract services related to WSO2 Public Clouds.

Do WSO2 Public Clouds use Sub Processors?
WSO2 Public clouds leverage subcontractors who provide us with certain tools listed in our WSO2 Subprocessor List.

Does WSO2 perform vendor security risk assessments (VSRAs)?
All suppliers, subcontractors, service providers, and vendors would be vetted by a team composed of IT, Security, Legal, HR, and Finance to ensure that external entities meet WSO2 standards. We would leverage vendors' security certifications, attestations, and security responses during the evaluation process.

Termination of Subscription

Can customers request a backup/copy of the data?

- *Asgardeo:*
  - *This can be facilitated via a support request for paid customers.*
- *Choreo:*
  - *No. Customers can 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 customer organization would get wiped out within 4 months.*

Contacting WSO2

How can customers 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/*