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.

Chroeo control plane

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

The workloads of Choreo subscribers are deployed on data planes.

Choreo cloud data plane

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

Choreo private data plane

Choreo subscribers can deploy their workloads on a private data plane hosted on a cloud service provider (CSP) such as Azure, AWS, or GCP or on an on-premises Kubernetes cluster. Private data planes offer more isolation and control of subscriber workloads. WSO2 can manage private data planes for subscribers on WSO2-owned or customer-owned subscriptions.

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. Customers enter their payment and billing information directly on Stripe when subscribing.

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 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.

Asgardeo

Type of data	Classification	Stored at	Purpose
Organization administrator profiles and associated data	Restricted	US deployment	User management
Business user profiles and associated data	Restricted	Regional deployments	User management
User roles/scopes	Restricted	Regional deployments	Privilege management
Secrets (keys/tokens/certificates)	Restricted	CSP 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
User profiles and associated data	Restricted	Asgardeo US deployment	User management
User roles/scopes	Restricted	Choreo control plane	Privilege management
Secrets (keys/tokens/certificates)	Restricted	CSP 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 facilitate service and legitimate interest (audit logs)

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.

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 customer data hosted?
WSO2 public clouds are hosted primarily on Microsoft Azure.

Where are the data centers located?

- *Asgardeo*
  - *Asgardeo organization administrator profiles and associated data would be stored in Asgardeo US deployment.*
  - *Asgardeo business 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 identity provider. Hence, user profiles and associated data would be stored in Asgardeo US deployment.*
  - *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 - customer's preferred data center region (AWS, Azure, GCP, OnPrem)*
- *WSO2 public cloud's billing and support portals are hosted in the US.*

Can customers 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, Asgardeo organization administrator profile data would be residing in the US. 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.*

Is customer 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 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.

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 support ticketing system and CRM for account management.*

How do WSO2 employees access the cloud infrastructure?
WSO2 leverages Azure 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.

From what locations do you access data?
Our DevOps, customer success, security, and account management teams are based in Sri Lanka, Brazil, the US, and the UK.

Technical and Organizational Controls

Cloud security

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

Data Encryption

What options are available for customers to encrypt their data?
We don't facilitate customers to encrypt their data. We leverage cloud service provider (CSP) technologies to encrypt customer data.

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

How is data encrypted at rest?
WSO2 utilizes CSP technologies such as disk and database encryption to encrypt data at rest.

How are Secrets encrypted?
Secrets are encrypted using CSP key vaults with CSP-managed keys.

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:*
  - *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*
  - *NoSQL database backups*
    - *Continuous, hourly, daily, weekly, monthly*
  - *Container registries and storage accounts are geo-redundant; Hence, they are not backed up separately.*

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 CSP-managed keys.

Can customers restore data if they need to?

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

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 in our 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 that 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 (e.g., 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 on our security page to report security vulnerabilities.

Internal Audits

The 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?

- *WSO2 public clouds (Asgardeo and Choreo) have successfully undergone a SOC 2 Type 1 audit, ensuring that our public clouds are designed to meet the control requirements of Security, Confidentiality, and Processing Integrity trust service criteria (TSC).*
    - *The audit covered controls of SOC 2 TSCs and HITRUST CSF controls that align with the SOC 2 TSCs.*
    - *We have obtained the SOC 2 Type 1 report with HITRUST CSF mapping.*
- *WSO2 is currently in the process of obtaining the SOC 2 Type 2 audit, and the SOC 2 Type 2 report will be available after Q4 2023.*
- *We will undergo annual audits to maintain the highest security and data protection standards.*

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 public clouds are not FedRAMP compliant and are included in WSO2's compliance roadmap.

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.

Are WSO2 public clouds PCI DSS certified?
WSO2 public clouds are not PCI-DSS compliant and are included in WSO2's compliance roadmap.

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 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 or copy of the data?

- *Asgardeo:*
  - *This can be facilitated via a support request for paid customers.*
- *Choreo:*
  - *No, customers 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 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/*

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.