



GENESYS CLOUD PLATFORM, SECURITY AND COMPLIANCE

Discussion White Paper

CVT (Global) Pty Ltd
December 2025

2 CONTENTS

1.1		0
3	Introduction	3
3.1	References	3
4	Platform	4
4.1	High Availability	4
4.2	Redundancy	6
4.3	Disaster Recovery	6
4.4	Scalability	7
4.5	References	7
5	Enterprise grade Security	8
5.1	About Genesys Cloud Security	8
5.2	Encryption	8
5.3	Authentication & SSO	9
5.4	System Hardening	9
5.5	Incident Response	9
5.6	References	9
6	Data	10
6.1	Storage	10
6.2	Sovereignty	10
6.3	GDPR	10
6.4	References	10
7	PCI DSS	11
7.1	References	11
8	Genesys Cloud Use of AI	13
8.1	Introduction	13
8.2	Understand Genesys Agent Copilot AI models, LLM input and AWS region mapping	13
8.3	A Comprehensive Guide to Genesys Cloud AI	13
8.4	Genesys Cloud AI Ethics	13
8.5	Genesys Cloud Privacy Policy Regarding AI Services	14
9	Genesys Cloud Compliance and Security Standards	15
9.1	Introduction	15
10	Further Genesys Cloud resources	16
10.1	Status and Uptime	16
10.2	Firewall, Bandwidth and QoS	16

11	Contact CVT.....	16
----	------------------	----

3 INTRODUCTION

Genesys Cloud delivers feature-rich services for collaboration, communications, and customer engagement. It's highly scalable, reliable, and secure, built on a true cloud Amazon Web Services (AWS), micro-services elastic architecture. Modern intuitive Web UI provides advanced routing of Omni channel interactions, speech enabled IVR, Recording & Quality Management, Social Channel & reporting.

This white paper has been put together by CVT (Global) Pty Ltd using information from the Genesys Cloud help centre and Genesys Cloud knowledge bases and is designed to provide an overview of Genesys Cloud's Platform and Security capabilities.

NOTE: As Genesys Cloud evolves, some information may be out-of-date. Please refer to the links to Genesys Cloud help centre for up-to-date information. All attempts have been made to verify the accuracy of this information however the final public reference should be the published material at the Genesys Help Centre, please contact your account manager for any clarifications.

3.1 REFERENCES

Please refer to these important sources of Genesys Compliance and Security articles and guidance:

Genesys Cloud Trust Site: <https://www.genesys.com/trust-center>

Genesys Security and Compliance Resources: <https://help.mypurecloud.com/articles/about-security-and-compliance/>

Guide to Genesys Cloud AI: <https://www.genesys.com/en-gb/resources/a-comprehensive-guide-to-genesys-cloud-ai>

4 PLATFORM

4.1 HIGH AVAILABILITY

The Genesys Cloud suite of application services is based on a new distributed cloud architecture built atop AWS. Genesys Cloud utilizes AWS services to provide highly available environments, including, but not limited to, the following:

- Genesys Cloud uses Elastic Load Balancers (ELBs) to route internal and external traffic to healthy servers. ELBs are clusters of servers that run in multiple availability zones. ELBs load balance HTTP requests across multiple availability zones and backend Elastic Compute Cloud (EC2) instances. When the ELB detects that a backend instance is either at capacity or has failed, it routes traffic to other instances in seconds to compensate. Both Genesys Cloud's public APIs and backend instances are fronted by ELBs.
- Genesys Cloud uses Availability Zones (AZs) which are geographical locations engineered to be insulated from failures in other AZs. Each AZ consists of one or more discrete data centres, each with redundant power, networking, and connectivity, housed in separate facilities. Dedicated fibre lines connect AZs so that normal connectivity has very low latency and AZ outages are detectable in seconds. All Genesys Cloud services are deployed into multiple AZs making them tolerant in the event of a data centre or even entire AZ failure.
- Genesys Cloud uses of Amazon Simple Storage Service (S3) providing a durable infrastructure to store important data and is designed to deliver eleven 9's of durability. Your data is redundantly stored across multiple facilities and multiple devices in each facility. Amazon S3 is designed for up to 99.99% availability of objects over a year and is backed by the Amazon S3 service level agreement. This ensures that the service is reliable.
- Genesys Cloud has more than 100 microservices running on Amazon Elastic Compute Cloud (EC2). Each microservice instance runs on its own EC2 instance, and each microservice has at least two instances running in separate AZs. Amazon ELBs load balance requests across the microservice instances and detect failed instances within seconds, routing requests to other instances. The EC2 instances are also in Amazon Auto Scaling groups, which scale up the number of instances to meet demand automatically and replace failed instances with new healthy instances in minutes.
- Genesys Cloud uses multiple cache clusters for caching data from databases and external services to make Genesys Cloud responsive. The nodes in each cluster spread across multiple AZs so that the loss of a single AZ does not bring down the cluster. If any node in the cluster fails, then the other nodes take over the failed node's work in seconds. If a complete cache cluster fails, then the cache cluster can be redeployed and begins caching data from the data's home of record in minutes.
- In addition to the database clusters, Genesys Cloud makes heavy use of DynamoDB. DynamoDB is highly available, with automatic and synchronous data replication across three facilities in a region. This helps protect your data against individual machine failures or even facility-level failures. All the Genesys Cloud DynamoDB tables are backed up hourly to S3 to ensure data restoration in hours in the event of a catastrophic failure.
- Genesys Cloud AI Services run in the Core region of the customers Genesys Cloud Org, for Australia homed Orgs this is AWS Australia region

Asia Pacific (Sydney)	ap-southeast-2	Asia Pacific (Sydney)
-----------------------	----------------	-----------------------

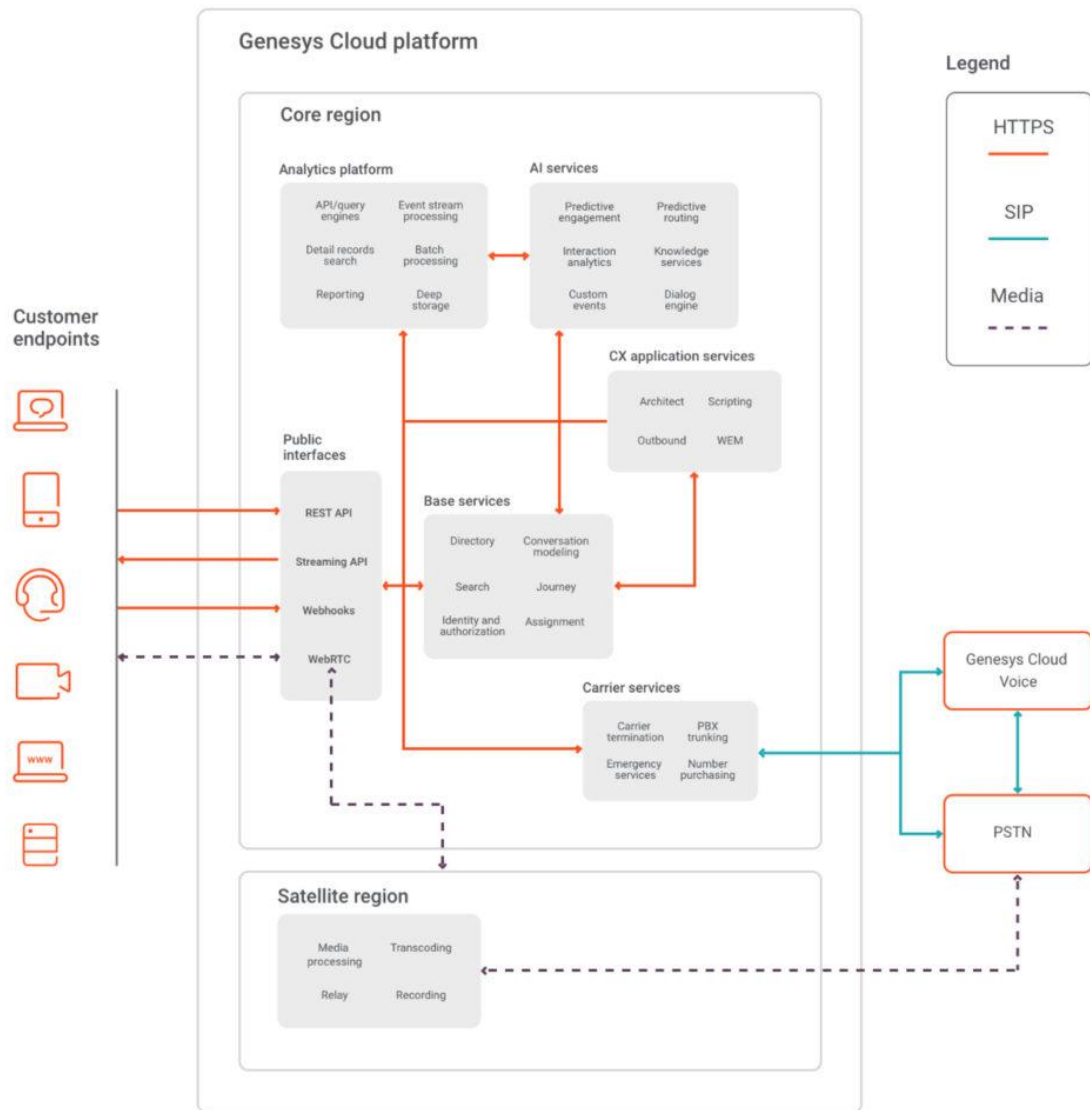


Figure 1: Genesys Cloud Platform Architecture

4.2 REDUNDANCY

Genesys Cloud takes advantage of Amazon's Availability Zones (AZs), which are engineered to be insulated from failures in other AZs. By placing Amazon EC2 instances in multiple AZs, an application can be protected from failure at a single location. The solution is architected to run independent application stacks in more than one AZ so that if one zone fails, the application in the other zone can continue to run. As standard, an organization runs in multiple AZs.

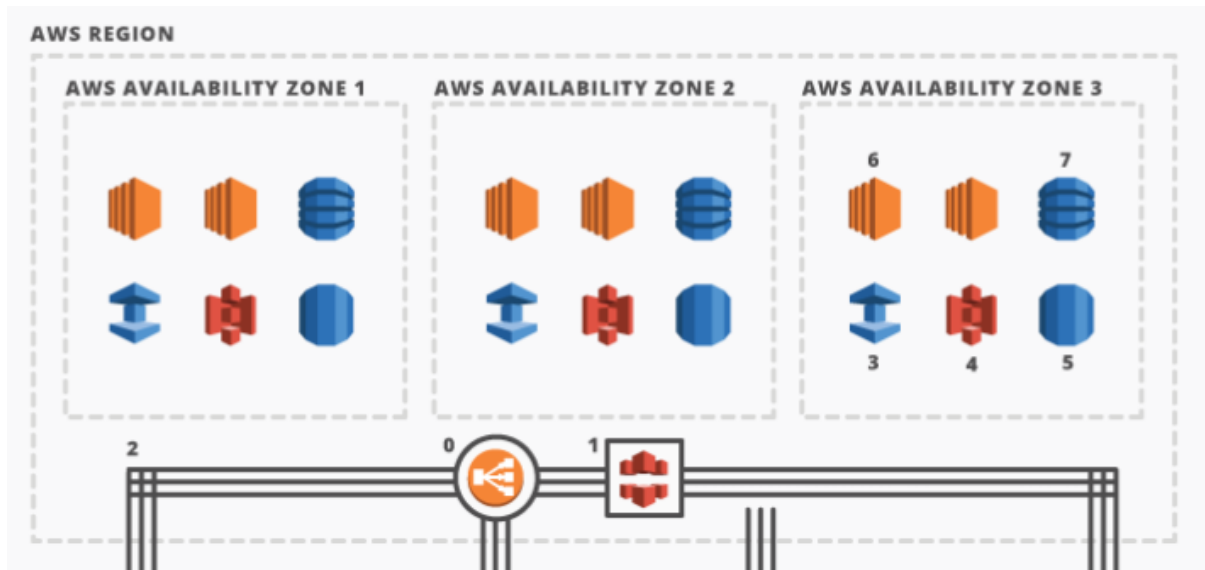


Figure 2: Genesys Core Redundancy

4.3 DISASTER RECOVERY

The Genesys Cloud platform takes advantage of the distributed nature of AWS infrastructure to enable full active-active Multi-Site Disaster Recovery by operating in multiple Availability Zones (AZ); distinct locations that are engineered to be insulated from each other. Independent application stacks are run in multiple AZs. In the event of the loss of a single AZ or data centre, the remaining Genesys Cloud systems remain operational and are designed to auto-scale to replace the lost system capacity, effectively ensuring a Recovery Time Objective (RTO) of zero. Genesys Cloud tests this on a regular basis with Chaos Testing.

4.4 SCALABILITY

Genesys Cloud provides the ability to dynamically add and remove resources as needed by leveraging AWS Elastic Load-Balancing (ELB) and Auto-Scaling Groups (ASG). Genesys Cloud distributes load and monitors groups according to service-specific policies (CPU for compute-intensive services, mean response time for a query service, and so on). Genesys Cloud does not have the limitation of only having X amount of physical machines to perform all its functions. If the system needs to process an unusually large chunk of data, Genesys Cloud can instantly spin up as many servers as it takes to handle the load, and then spin them back down again when they are no longer needed. For example, if an organization suddenly needs to send a million faxes, the associated microservices automatically scale out to meet the demand without impacting other functionality or other tenants.

4.5 REFERENCES

What is Genesys Cloud? <https://help.mypurecloud.com/articles/genesys-cloud/>

Overview of Architecture and technology: <https://help.mypurecloud.com/articles/about-architecture-and-technology/>

Genesys Cloud Platform: <https://help.mypurecloud.com/articles/about-the-genesys-cloud-platform/>

Microservices: <https://help.mypurecloud.com/articles/microservice/>

Genesys Cloud Trust Site: <https://www.genesys.com/company/trust/>

5 ENTERPRISE GRADE SECURITY

5.1 ABOUT GENESYS CLOUD SECURITY

Security and operational controls are based on industry standard practices and are certified to meet HIPAA, PCI Service Provider Level 1, and SSAE16 Service Organization Control (SOC) 2 Type II/ISAE 3402 guidelines. Genesys Cloud utilizes infrastructure deployed on Amazon Web Services (AWS). AWS provides the following letters of compliance and/or certification: ISM, ASD, ISO 9001:2008, ISO 27001:2013, ISO 27018:2014, ISO 27017:2015, Multi-Tier Cloud Security Standard Level-3 (CSP) Certification. AWS also undergoes frequent SOC 3 audits. A copy of the certifications and audit reports for AWS are available on the AWS website at <http://aws.amazon.com/compliance/published-certifications>.

Genesys Cloud has completed a third-party SSAE 18 SOC 2 Type II examination. SSAE 18 conveys our commitment to the highest standards by providing Genesys Cloud customers with assurance of security and privacy controls. CSA and Australian Data Sovereignty is also compliant. Nevertheless, the customer is solely responsible for achieving and maintaining any industry specific certifications required for your business (e.g., PCI DSS, HIPAA).

5.2 ENCRYPTION

The Genesys Cloud solution leverages TLS for information transiting the public internet, and increasingly within our backend VPC. Sensitive data such as call recordings are encrypted at the point of recording with customer-specific keys, doubly encrypted in transport with TLS 1.1 and above, and again doubly encrypted at REST with Amazon S3 Server-side encryption.

Genesys Cloud's encryption algorithm uses strong 3072-bit public/private key pairs to create unreadable records that may be safely stored off-premises. The use of long and strong cryptographic keys provides an effective defence against brute force attacks. Public and private keys in a pair are mathematically linked. The private key is used to decrypt anything encrypted by its corresponding public key.

Encryption key updates

Encryption keys can be changed on a scheduled rotation, controlled within the Genesys Cloud interface. Changing encryption keys regularly helps ensure the safety of your recorded interactions by limiting the number of recordings that a given key can access.

Encryption in Transit:

- Encrypted data connections: All connections to browsers, mobile apps, and other components are secured via Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS) over public Internet.
- Encrypted call recordings and faxes: Genesys Cloud ensures the security of communications by encrypting call recordings and faxes over public Internet.

Encryption at Rest:

- Sensitive objects are encrypted at rest using Server-Side Encryption (AES-256), which include
 - Interaction Recordings – Voice, Chat, Email, SMS and Messaging
 - External Contacts and Documents

5.3 AUTHENTICATION & SSO

All passwords are hashed using a salt with SHA-512 combined with PBKDF2. These cryptographic methods make Genesys Cloud extremely resilient to rainbow table attacks.

SSO and Multi-Factor Authentication (MFA) are supported via third-party integration. Location based restriction is supported through some third parties. Genesys Cloud currently supports Google G Suite, Ping Identity, Microsoft Azure AD Premium, Microsoft Active Directory Federation Services (ADFS), OneLogin, OKTA and Salesforce as identity providers.

About SSO: <https://help.mypurecloud.com/articles/about-single-sign-on-sso/>

5.4 SYSTEM HARDENING

The Genesys Cloud operating system hardening is done by starting with the latest release of Amazon Linux, next building a derived base Amazon Machine Image (AMI) from that release, and then configuring the operating system as follows:

- Install all Amazon Linux security and normal updates
- Remote access via Secure Shell (SSH) only and using SSH keys rather than passwords
- Installing ThreatStack and AlertLogic

The Base AMI is rebuilt weekly, and via our deployment tools we enforce a service cannot deploy with an AMI that is based on a base AMI older than 30 days, which ensures that services are no more than 30 days out-of-date on all security updates.

5.5 INCIDENT RESPONSE

Genesys has implemented an incident response program based on industry best practices. The goal of the incident management program is to minimize the adverse impact of incidents resulting from issues within the Genesys environment and to prevent the recurrence of incidents related to those issues. It is designed to identify, contain, and eradicate the root cause of incidents through investigation and analysis. Upon identification of the root cause, the Security Incident Response Team (SIRT) is a cross disciplinary team within Genesys that works to eradicate the issue and implements corrective and preventive actions with the appropriate team members to resolve the underlying problem, thus reducing the likelihood of recurrence. The program is overseen by Information Security but involves subject matter experts from across the organization, and supplemental experts are available to assist where necessary. These might include changes to internal processes, procedures, and/or infrastructure.

5.6 REFERENCES

Genesys Cloud Security and Compliance overview: <https://help.mypurecloud.com/articles/about-security-and-compliance/>

Genesys Cloud Security policy: <https://help.mypurecloud.com/articles/genesys-cloud-security-policy/>

6 DATA

6.1 STORAGE

Customer data is stored in several places within Genesys Cloud. Each microservice within Genesys Cloud "owns" its data tier, with access to it only via API. This allows Genesys Cloud to enforce granular access control policies despite having disparate data technologies and multitenancy.

6.2 SOVEREIGNTY

Unless otherwise specified, CVT uses the Australian region for Genesys Cloud and therefore all Genesys Cloud data is located within Australia.

6.3 GDPR

In Genesys Cloud's role as a data processor, Genesys Cloud has taken measures to meet the requirements of GDPR regulations. Genesys Cloud provides a GDPR API as the preferred self-service solution for Genesys Cloud customers to respond to GDPR requests. Genesys is Privacy Shield certified for transfers to the United States and uses Standard Contract Clauses for any transfers to other non-adequate regions.

No GDPR certification exists for a cloud services provider such as Genesys Cloud. However, Genesys Cloud has undergone multiple independent reviews of our administrative, physical, and technical controls for other data protection regulations, such as HIPAA.

The Genesys Cloud GDPR API completes most search requests (GDPR_EXPORT) within two days. For full, up-to-date information about the GDPR and Genesys Cloud GDPR compliance support, see

6.4 REFERENCES

GDPR: <https://help.mypurecloud.com/articles/gdpr-compliance/>

GDPR: <https://help.mypurecloud.com/articles/genesys-cloud-and-gdpr-compliance/>

7 PCI DSS

Genesys Cloud's PCI DSS compliance has been validated by an external Qualified Security Assessor (QSA) and is Service Provider Level 1 compliant with PCI DSS version 3.2.

The Genesys Cloud PCI DSS feature set includes the LUHN algorithm, Secure Pause and Secure Call Flows to comply with PCI DSS requirements.

Luhn: Genesys Cloud automatically prevents itself from transferring or storing credit card numbers as is required for certain organizations that must meet specific regulatory or industry standards such as PCI DSS. Genesys Cloud uses filtering to prevent the transmission of credit card numbers between users and agents. Genesys Cloud also uses filtering to prevent the storing of credit card numbers received through ACD Email. The Genesys Cloud filtering is based on the Luhn algorithm and related to ISO/IEC 7812-1:2017.

Secure pause: When activated, Secure Pause temporarily stops recording to exclude sensitive information, such as entry of a credit card number. Before receiving cardholder data using Genesys Cloud, an agent must always initiate Secure Pause to stop recording. After receiving cardholder data, to resume recording the agent must deactivate Secure Pause.

Secure Call Flow: When activated, a secure flow temporarily prevents system recording or agent access to a caller's entry of sensitive information, such as cardholder data. Before receiving cardholder data using Genesys Cloud, an agent must transfer a call to a Secure Flow. After cardholder data has been received, the call may be transferred back to the agent.

Both Secure Pause and Secure Call Flows are certified for PCI Compliance with either local Edge devices or with virtual edges and Genesys Cloud Voice in any deployment region.

PCI DSS Setting: When enabled, PCI DSS-compliant organizations disable the logging of DTMF and media capture by the Edge.

7.1 REFERENCES

Overview: <https://help.mypurecloud.com/articles/pci-dss-compliance/>

LUHN: <https://help.mypurecloud.com/articles/sensitive-information-filtering/>

Secure Pause: <https://help.mypurecloud.com/articles/pause-interactions-recording-protect-sensitive-information/>

Secure Call Flow: <https://help.mypurecloud.com/articles/secure-call-flows/>

Is your Genesys Cloud automatically PCI DSS compliant using these features?

Your Genesys Cloud implementation design, coupled with your responsibilities as the end customer will affect your PCI DSS compliancy.

The implementation design - whether your edge devices are fully hosted, on-prem or hybrid will influence your PCI DSS capacity. Please enquire to which design model applies for your Genesys Cloud.

Furthermore, as the customer, you and Genesys Cloud share responsibilities for operating Genesys Cloud in a PCI DSS-compliant manner. Please see the customer responsibility matrix for further details: <https://help.mypurecloud.com/articles/pci-dss-customer-responsibility-matrix/>

8 GENESYS CLOUD USE OF AI

8.1 INTRODUCTION

Genesys utilises AI related features in a number of functional areas of Genesys Cloud, as an integral function of the Genesys Cloud service the AI features follow the overall platform security and compliance outlined in this document including services and associated data being run and stored in the same region as the Genesys Org, for Australia customers this is Australia AWS Region only.

About Genesys Cloud AI: <https://help.mypurecloud.com/articles/about-genesys-ai/>

8.2 UNDERSTAND GENESYS AGENT COPILOT AI MODELS, LLM INPUT AND AWS REGION MAPPING

Genesys Agent Copilot uses a combination of Genesys native and AWS Bedrock models, depending on the feature, use case, and dialect. These models run in the same AWS region as the Genesys Org tenancy, in the case of Australia this is Australia.

Further details on models and LLM input: <https://help.mypurecloud.com/articles/understand-genesys-agent-copilot-ai-models-and-llm-input/>

8.3 A COMPREHENSIVE GUIDE TO GENESYS CLOUD AI

Customer and employee expectations are changing. To remain competitive, businesses need the ability to innovate and easily adapt to these shifting demands. Our AI-powered Genesys Cloud™ platform can help you transform those experiences now — and into the future.

This guide offers a clear and high-level overview of Genesys Cloud AI to help you gain more visibility into how our models are trained, how data is used and secured, and our stance on AI ethics. We'll answer common questions and share some additional resources and insights into how some Genesys customers are using AI to gain a competitive advantage.

Get the Guide: <https://www.genesys.com/en-gb/resources/a-comprehensive-guide-to-genesys-cloud-ai>

8.4 GENESYS CLOUD AI ETHICS

Genesys is committed to building responsible AI that enhances customer experiences while upholding privacy, fairness, transparency and security. This article outlines our ethical framework for AI development and deployment, which is guided by four foundational principles: Accountability, Security and Privacy, Transparency, and Fairness. These pillars guide how we build, govern, and evolve AI in ways that are responsible, trustworthy and align with customer values. Through robust governance, clear controls and ongoing improvement, we aim to ensure our AI systems are trustworthy, compliant and beneficial for all users.

Read the Article: <https://www.genesys.com/article/genesys-cloud-ai-ethics>

8.5 GENESYS CLOUD PRIVACY POLICY REGARDING AI SERVICES

Privacy by Design and Privacy by Default are embedded in the processes around the design, set up and update of our products and services — from development to release and improvement. Our standard baseline for compliance with privacy and data protection is the EU General Data Protection Regulation (GDPR) and related legislative pieces, which are foundational for our privacy program.

In addition to that, our risk management framework incorporates AI model actions, including privacy as a pillar. Our corporate and product privacy teams are knowledgeable of other AI risk frameworks incorporating privacy to the assessment of AI products, such as the NIST AI Risk Management Framework, ISO/IEC 23894:2023, and additional resources such as the Assessment List for Trustworthy AI developed by the High-Level Expert Group on AI set up by the European Commission. This provides a robust framework designed to protect fundamental rights from the design phase of AI models.

Here are additional details about the Genesys position on privacy and compliance:

- Building large-scale systems that apply AI to optimize customer experience often requires very large datasets that can contain data on many individuals coming from a variety of sources. Genesys is committed to core principles of privacy by design, limiting the data collected about individuals as the default.
- Beyond enforcing privacy by design principles across systems, Genesys uses rigorous processes to monitor compliance of our AI products with regulations such as GDPR and any other applicable legislation globally.
- While Genesys has technical and administrative controls in place to limit the access to customer data, we have established additional safeguards designed to ensure that all data used for the development of new products is anonymized and governed by a set of processes detailed in the Genesys data anonymization framework.

Genesys Privacy Policy Regarding AI: <https://help.mypurecloud.com/faqs/what-is-your-privacy-policy-regarding-ai-services/>

9 GENESYS CLOUD COMPLIANCE AND SECURITY STANDARDS

9.1 INTRODUCTION

Genesys Cloud supports various industry standard security practices and operational controls, in the context of Australia this includes certification for Federal Government use under IRAP (Protected level).

Genesys Supported Security Standards: <https://help.mypurecloud.com/articles/supported-security-standards/>

Genesys Cloud Trust Centre: <https://www.genesys.com/trust-center>

10 FURTHER GENESYS CLOUD RESOURCES

10.1 HARDENING THE GENESYS CLOUD ENVIRONMENT AND SECURING 3RD PARTY APPS

Notes on securing 3rd party applications available here <https://www.genesys.com/blog/post/secure-third-party-apps-before-peak-demand-hits> includes link to details on hardening Genesys environment <https://help.mypurecloud.com/articles/harden-the-genesys-cloud-environment/>

10.2 STATUS AND UPTIME

For the current and historic status and uptime of Genesys Cloud, including AI related services please see the Genesys Cloud status page. Subscribe for real-time updates on status changes and incidents.

- <https://status.mypurecloud.com/>

10.3 FIREWALL, BANDWIDTH AND QOS

The below links provide an overview of the Firewall requirements relating to aspects of using Genesys Cloud. Please contact CVT for further documentation around technical requirements and specifications.

- **Firewall rule requirements**
 - <https://help.mypurecloud.com/articles/genesys-cloud-ports-services/>
 - For Telstra Genesys Cloud (TPC) please refer to *Genesys Cloud Voice*
 - For chat, screen recording - please refer to 'General' and 'Co-browse, chat, video chat, screen share, screen recording'.
 - <https://help.mypurecloud.com/articles/ports-and-services-for-webrtc/>
 - For WebRTC use. For Telstra Genesys Cloud refer to *Genesys Cloud Voice*
 - To test, please use WebRTC tester: <https://apps.mypurecloud.com/webrtc-troubleshooter/#/audio>
- **Voice and QoS policy**
 - <https://help.mypurecloud.com/articles/customer-network-readiness/>
 - Please refer to 'QoS settings'
- **Bandwidth**
 - The following calculator can also be used to help in estimating Voice and SIP bandwidth.
 - https://help.genesys.com/staging/edge_bandwidth_calculator/
 - For TPC: Please use Gateway 'Genesys Cloud Voice'

11 CONTACT CVT

Please contact CVT for any questions or clarifications.

- T: 1300 000 288
- E: sales@cvt.com.au
- W: <http://www.cvt.com.au>