Description of data processing – Genesys Cloud

Categories of Data Subjects

(i) Users authorised by you to use the Service ("**Authorised Users**") and any employees, agents, advisors, and other authorised representatives of Authorised Users; and/or

(ii) External persons connecting to your platform without an account, such as those receiving calls and instant messages ("**External Parties**").

Categories of Personal Data

Transfer (a): **User account and configuration details:** Details required to create Authorised Users' accounts, including first / last name, email address, unique identifier, phone numbers, and other configuration requirements as determined by the Customer, such as call routing information based on staff proficiency or skillsets.

Transfer (b): **Communications content and interactions:** Depending upon the features enabled by the Customer, this could include call recordings, voicemails, text messages, email, social media chat, and other interactions with External Parties over the platform. This involves the generation of unique identifiers to identify individual interactions.

Transfer (c): **Third party information for personalisation:** Depending on the access enabled by the Customer to its own platforms and its line of business, this could include information about External Parties, such as its customers or potential callers' name, date of birth, address, as determined by Customer, to personalise the service or triage the call.

Transfer (d): **Derived analytics information:** The platform has the ability to derive information from calls and messages, such as by spotting trends in transactions, enabling bots to chat via text messages, identifying key words and analysing sentiment to assist with call flow or agent selection, which may identify External Parties.

Transfer (e): **Workforce management information:** Agents' scheduled work time can be configured into the platform to monitor for real-time or historical adherence to schedules and manage other workforce scheduling requests.

Telstra does not collect or process any special categories of Personal Data as part of this service. Telstra does not have control over the communications content and data shared by Authorised Users and External Parties and relies on the Customer to ensure that the former do not disclose any special categories of Personal Data while using the Service. Customers are able to revoke configuration permissions at any time and, upon request, Customers are able to create a custom role for Telstra preventing Telstra from accessing and downloading call recording or conversation data.

While it is highly unlikely that Telstra personnel would, or could, view any Special Categories of Personal Data, Telstra is committed to further protecting this data by implementing additional controls such as: (a) including information in guidelines that the logs are only to be used for permitted purposes (i.e. in connection with the Service); (b) including guidance in the onboarding process for relevant new personnel; and (c) providing regular reminders to relevant personnel.

Nature of the processing, frequency of the transfer, and data retention periods

Transfer	**Nature of processing**	**Frequency**	**Data retention**
Transfer (a): User account and configuration details	Storage, remote access, and/or hosting by Telstra affiliates and personnel, or Subprocessor/s, as detailed in this document, to configure the platform, and provide troubleshooting, management and assurance.	Continuous storage; access on an as needed basis	As determined by Customer on the Genesys Platform
Transfer (b): Communications content and interactions	Storage and hosting by the Subprocessor listed in this document. Access by Telstra affiliates and personnel for troubleshooting and assurance.	Continuous storage; access on an as needed basis upon request from the Customer	As determined by Customer on the Genesys Platform
Transfer (c): Third party information for personalisation	Access by the Subprocessor listed in this document and by Telstra affiliates and personnel for troubleshooting, assurance and improving the service.	Continuous storage; access on an as needed basis upon request from the Customer	As determined by Customer on the Genesys Platform

Transfer (d): Derived analytics information	Storage and hosting by the Subprocessor listed in this document. Access by Telstra affiliates and personnel for troubleshooting and assurance.	Continuous storage; access on an as needed basis upon request from the Customer	As determined by Customer on the Genesys Platform
Transfer (e): Workforce management information	Storage and hosting by the Subprocessor listed in this document. Access by Telstra affiliates and personnel for troubleshooting and assurance.	Continuous storage; access on an as needed basis upon request from the Customer	As determined by Customer on the Genesys Platform

Technical and organisational measures to ensure the security of the Personal Data

Telstra protects all third country transfers of Personal Data, undertaken by Telstra personnel or affiliates as detailed in this document, in accordance with our suite of information security standards. These standards define a number of baseline controls, which are implemented at appropriate risk based levels to protect the confidentiality, integrity and availability of both Telstra core and customer specific data. The controls and practices detailed in the standards align to industry practices and standards, such as ISO/IEC 27001:2013, ISO 31000:2009, NIST and PCI DSS. Telstra can provide details of our current certifications upon request from customers.

Telstra conducts periodic reviews of the information security standards, and may therefore amend the below baseline controls from time to time to align with industry security standards and the evolving risk landscape:

Standard	Practices
Access Control	**User access responsibilities:** Telstra staff are only able to use approved, authenticated, and encrypted remote access communication methods to log into Telstra's network and access any Network User and Authorised User Personal Data. **Identification:** Telstra users are granted a unique ID before being granted access to any systems containing Network User and Authorised User Personal Data, so that access is logged and monitored. **Role assignment and role based access control:** Telstra implements and maintains system and application access profiles based on the principle of least privilege, which means that staff are only provided with the minimum access to Network User and Authorised User Personal Data required to perform their role. This includes record-keeping of authorised system users with access to Network User and Authorised User Personal Data and governance procedures around these records, such as the annual revalidation or certification of user access requirements.

Standard	Practices
	Passwords and authentication mechanisms: Telstra uses authentication methods that are capable to validating passwords in-line with Telstra's standards for password strength and complexity. Passwords are also encrypted at rest.
Application Security	**Developer training and awareness:** Software developers are trained on foundational concepts for building secure software including secure design, threat modelling, secure coding, security testing, and best practices surrounding privacy. **Application design:** Telstra requires that applications are signed to disabling or restrict access to system services, applying the principle of least privilege, and employing layered defences wherever possible. This includes a requirement that all third-party software is securely configured to recommended vendor security configuration, or Telstra standards, and applying strict controls around access to repositories containing Telstra source code.
Change and Configuration Management	**Process and procedures:** Telstra does not permit Network User and Authorised User Personal Data to be used for development purposes – non-production and production environment must be separated and, at a minimum, enforce logical isolation. **System and server configuration:** Telstra maintains security configuration baselines consistent with industry accepted hardening standards, which address known security vulnerabilities, and communicates these to relevant personnel. Servers are specifically configured to prevent Network User and Authorised User Personal Data from being exported to unauthorised users.
Cryptography	**Cryptographic algorithms:** Only Telstra approved algorithms may be used, and Telstra requires that system configuration support is removed for all weak, non-approved algorithms. Access to encryption keys is recorded and audited at least annually.
Data Protection	**Information classification:** Network User and Authorised User Personal Data is classified as such to meet applicable requirements under data protection laws. This enables Telstra to remove Network User and Authorised User Personal Data from datasets, if not required to provide the agreed service or meet regulatory requirements, and to remove or protect direct identifiers of Personal Data in datasets, using approved algorithms or software. **Information handling:** Telstra staff must protect Network User and Authorised User Personal Data by using approved encryption methods when it is been stored and transmitted, only using authorised file sharing services, and locking devices when not in use. At an application level, Telstra solutions must meet data segregation requirements, so that each customer's data is logically separated from other customers' data and users can only see customer data that they require for their role.
Incident Management	**Incident response plan:** Telstra maintains and tests an incident response plan, which is supported by the designation of personnel who are available

Standard	Practices
	on a 24/7 basis to respond to alerts, along with training to all staff with security breach response responsibilities.
Logging and monitoring	**Audit log content and trails:** Telstra implements audit trails that link system component access to individual user accounts to reconstruct access to Network User and Authorised User Personal Data. Logs for systems that store, process, or transmit Network User and Authorised User Personal Data are continually reviewed.
Network security	**Network management:** Telstra operates procedures for monitoring access to network resources and sensitive data environments, and uses intrusion detection / prevention techniques on traffic entering its internal network.
Physical security	**Facility controls:** Telstra limits and monitors physical access to systems containing Network User and Authorised User Personal Data by requiring that access is authorised and based on individual job functions, any third party access is vetted and approved, and access is revoked immediately upon termination. **Data centre physical access:** Telstra restricts entry into server rooms and protects against unauthorised access by logging entry and exit, requiring a special code or key for entry, and configuring access controls to continue preventing unauthorised entry if power is lost.
Staff security	**General security culture and conduct:** Telstra maintains a formal security awareness program so that staff are aware of their security responsibilities. This includes providing an annual security module to all staff and additional role-based training for relevant personnel. **Background checks:** Telstra staff undergo relevant and appropriate background checks.
Supplier Management	**Due diligence:** Telstra requires that a partner security assessment is undertaken for suppliers that have the potential to access Network User and Authorised User Personal Data. **Contracts:** In addition to clauses required under data protection laws, Telstra incorporates standard data security clauses into contracts for suppliers that will access, transmit, use, or store Network User and Authorised User Personal Data. **Security:** Suppliers must agree to comply with Telstra security standards and any additional Telstra requirements for the secure access, exchange, and lifecycle management of Telstra information, including Network User and Authorised User Personal Data; data loss prevention; and business continuity and disaster recovery.
Vulnerability management	**Vulnerability protection:** Telstra deploys anti-malware software, penetration testing, vulnerability assessments, and periodic evaluations of malware threats to systems. **Patch management:** Telstra requires that system components and software are patched and protected from known vulnerabilities, and controls are in place to verify the integrity of patches prior to deployment.

Telstra has implemented technical and organisational measures and processes to comply with data subject rights as further detailed in Telstra's privacy statement, available at Tel.st/privacy-policy.

In addition to the supplier management controls detailed above, Telstra also employs specific technical and organisational measures to ensure that Subprocessors, as detailed in this document, are able to provide assistance in meeting obligations under relevant Applicable Data Protection Laws. These include:

- Security and operational controls based on industry standard practices and certified to meet the guidelines of PCI, SOC 2 Type 2, ISO 27001, and HIPAA.
- Information security and awareness programs are in place and re-delivered annually
- Logical separation controls based on industry standards are used to ensure that customer data is logically separated from other customer data within cloud services environment
- The deployment spans across separate data centres providing optimal availability of the cloud services and leverages the distributed nature of the infrastructure to enable full multi-site disaster recovery by operating in multiple availability zones.
- Access controls are implemented to ensure that only authorised Telstra user accounts have access to Customer data within the cloud environment.

List of Subprocessors

Telstra has engaged the following Subprocessors:

- Genesys Telecommunications Laboratories Inc for Transfer (a): User account and configuration details; Transfer (b): Communications content and interactions; Transfer (c): Third party information for personalisation; Transfer (d): Derived analytics information; Transfer (e): Workforce management information

These include applicable Telstra affiliates listed here, as updated from time to time.

Contact person details and address of the listed Subprocessors, are available upon request to Telstra at privacy@online.telstra.com.au.