Description of data processing – SIP Connect Reseller

Categories of Data Subjects

(i) Current, prospective and former clients and customers of you ("**Clients**") and employees, agents, advisors, and other authorised representatives of Clients.

Categories of Personal Data

Transfer (a): **Billing portal data:** If Telstra provides Clients with access to our password protected billing portal, we may transfer records contained in this portal, which relate to these Data Subjects, including caller line identity, dialed numbers, call duration, IP address, and estimated usage costs;

Transfer (b): **Porting data:** As part of the number porting process, we may transfer the details of a designated individual of a Client to a Subprocessor, as detailed in this document, at the Client's written request. These details may include contact person's first/last name, business registration number, work email, reason for port, use of number, signature, and/or company stamp;

Transfer (c): **Customer registration details:** These details depend on the country where the service is operating and will typically include Client's contact person's name, business registration number, work email, reason for use of number, signature, and/or company stamp;

Transfer (d): **Call Data Records** ("**CDRs**")**:** CDRs capture details about calls, including caller line identity, dialed number, type of call, call connect time, call duration, a Telstra unique identifier used to calculate billing data, call type, call protocol, source and destination registered IDs for the call flow, and source IP address; and/or

Transfer (e): **End user details:** For compliance with regulatory requirements, such as obligations related to emergency calling and geolocation services, we may transfer the details of all Clients, or a designated individual of a Client, including full name, assigned number and address, in accordance with each country's requirements.

Telstra does not collect or transfer any special categories of Personal Data as part of this service.

The parties acknowledge that Telstra is a mere conduit with respect to the contents of communications data sent and received using the services and that as such Telstra does not Process any Personal Data comprised in the contents of communications data, either as a Controller or a Processor.

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

Transfer	Nature of processing	Frequency	Data retention
Transfer (a): Billing portal data	Storage and hosting by the Subprocessor listed in this document for the purpose of providing Clients with access to a billing portal. Access by this Subprocessor and Telstra personnel and/or affiliates.	Continuous storage and hosting; access on an as needs basis	Up to 24 months, or in accordance with applicable law and as otherwise agreed with Clients for record-keeping purposes.
Transfer (b): Porting data	Transferred to a Subprocessor, as detailed in this document, for port in or port out requests.	On an as needed basis upon request	Determined by the Subprocessor, in accordance with applicable law and standards in the recipient jurisdiction.
Transfer (c): Customer registration details	Storage and remote access by Telstra personnel and/or affiliates, and the Subprocessor outlined in this document, for port in or out requests, new provisions, terminations, assurance support, and service monitoring.	Continuous storage; access on an as needed basis	Up to seven years, or in accordance with applicable law and as otherwise agreed with Clients for record-keeping purposes.
Transfer (d): CDRs	Storage and remote access by Telstra affiliates, along with transfers to Subprocessors per this document, to bill usage, for assurance support, and to provide Clients with	Continuous storage; access on an as needed basis	Up to 24 months in a readily accessible format by our billing Subprocessor listed in this document; Telstra internal systems store raw data for monthly periods, depending on system needs,

	access to their CDRs.		and Telstra internal archives are kept up to seven years, or in accordance with applicable law and as otherwise agreed with Clients for record-keeping purposes.
Transfer (e): End user details	Transferred to Telstra affiliates for compliance with regulatory requirements, such as obligations related to emergency calling and geolocation services.	On an as needed basis upon request	Determined by the Subprocessor, in accordance with applicable law and standards in the recipient jurisdiction.

Technical and organisational measures for ensuring the security of 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 Client personal data. **Identification:** Telstra users are granted a unique ID before being granted access to any systems containing Client 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 Client Personal Data required to perform their role. This includes record-keeping of authorised system users with access to Client Personal Data and governance procedures around these records,

Standard	Practices
	such as the annual revalidation or certification of user access requirements. **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 Client Personal Data to be used to 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 all known security vulnerabilities, and communicates these to relevant personnel. Servers are specifically configured to prevent Client 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:** Client Personal Data is classified as such to meet applicable requirements under Applicable Data Protection Laws. This enables Telstra to remove Client 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 Client 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 Client Personal Data. Logs for systems that store, process, or transmit 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 Client 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 unathorised access by logging entry and exit, requiring a special code or key for entry, and configuring access controls to continue preventing unathorised 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 Client Personal Data. **Contracts:** In addition to clauses required under Applicable Data Protection Laws, Telstra incorporates standard data security clauses into contracts for suppliers that will access, transmit, use, or store Client 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 Client 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 the relevant Subprocessors are able to provide assistance in meeting obligations under Applicable Data Protection Laws. These include:

- Access by Subprocessors involved in Transfer (d): CDRs occurs behind Telstra firewalls, on Telstra premises, thereby applying the above controls relating to Telstra's security environment.
- Where possible, access undertaking as part of Transfer (d): CDRs utilises a pseudenoymised unique PIN to identify Clients' end users, both internally and with relevant Subprocessors.
- User identification and authorisation controls are applied for Subprocessors with continuous access to data, as detailed in Annex I.B, so that access is controlled, only granted to authorised individuals, and removed once that individual no longer needs access to the relevant system.
- The Subprocessor involved in Transfer (a): Billing portal data applies ISO 27001 standards. Data is also segregated and protected by access control, network access lists, firewalls, including when this Subprocessor partakes in Transfer (d): CDRs.

List of Subprocessors:

Telstra has engaged the following Subprocessors:

- MIND CTI Ltd. for Transfer (a): Bill portal data; Transfer (d): CDRs
- Ribbon Communications International Limited (contracted via Westcon International Limited) for Transfer (d): CDRs
- CSG International Pty Ltd for Transfer (d): CDRs
- Infosys Technologies Limited for Transfer (d): CDRs
- Infosys BPO Limited for Transfer (b): Porting data; Transfer (c): Customer Registration Details
- Metaswitch Networks Ltd (contracted via Microsoft Corporation) for Transfer (d): CDRs
- Capgemini Australia Pty Ltd for Transfer (d): CDRs
- Tata Consultancy Services Limited for Transfer (d): CDRs
- Titanium Platform LLC (contracted via Microsoft Corporation and Metaswitch Networks Ltd) for Transfer (d): CDRs
- AMAZON WEB SERVICES for Transfer (c): Customer registration details

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.