Description of data processing – IoT Global Connect (IGC)

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.

(ii) Where you are an authorised reseller, we may Process Personal Data relating to current, prospective and former clients and customers of you ("**Reseller Clients**"), subject to your operating model and onboarding processes.

Categories of Personal Data

Transfer (a): **Customer registration details:** In order to create the accounts and provide access to the portal we may process details typically including Authorised User's and, if applicable, Reseller Clients' first name and surname, ID number, contact person's name and surname, phone and email, and delivery addresses to fulfil orders for physical SIM card delivery.

Transfer (b): **Portal configuration and activity:** Captures details about Authorised Users and Reseller Client activity and configurations, such as details of changes made by individual users, detail of the change and the relevant date, and actions to trigger events based under subscription packages.

Transfer (c): **Application Programming Interface (API) Request information**: Upon your request to integrate with your own platform or to perform bulk requests via API instead of through the graphical user interface, we or Subprocessor (1) listed in Annex III may log authentication requests, change password requests, and user management or role management requests. These may include user ID, time of request, originating IP address, session information, and any other data included in the API.

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 by the machine to machine SIM cards using Telstra's IoT Global Connect (IGC) 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): Customer registration details	Hosting, storage, and remote access by the Subprocessors listed in this document and by Telstra personnel and/or Affiliates for the purpose of providing Authorised Users and Reseller Clients with access to the portal and undertake billing.	Continuous hosting and storage; and access on an as needed basis	Within 15 days upon Customer's request, or automatically upon deletion of user account. Other personal data is held up to 7 years in compliance with applicable legal or regulatory requirements
Transfer (b): Portal configuration and activity	Hosting and storage by Subprocessor (1) as detailed in this document and access by Telstra personnel and/or Affiliates to provide network and platform operational support and assurance, facilitate customer discussions, product development and design.	Continuous hosting and storage, and access on an as needed basis	Basic user account information is deleted immediately after a user is deleted. Other Personal Data is held for up to 7 years in compliance with applicable legal or regulatory requirements years
Transfer (c): Request via the Application Programming Interface (API)	Hosting and storage by the Subprocessor (1) as detailed in this document and access by Telstra personnel and/or Affiliates to execute platform integration and API requests.	Continuous hosting and storage, and access on an as needed basis	Up to 3 years in compliance with applicable legal and regulatory requirements.

Technical and organisational measures to ensure 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 Personal Data. **Identification:** Telstra users are granted a unique ID before being granted access to any systems containing 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 Personal Data required to perform their role. This includes record-keeping of authorised system users with access to Personal Data and governance procedures around these records, 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 Personal Data to be used for development purposes – non-production and production environment must be separated and, at a minimum, enforce logical isolation.

Standard	Practices
	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 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:** Personal Data is classified as such to meet applicable requirements under data protection laws. This enables Telstra to remove 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 r 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 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 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 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

Standard	Practices
	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 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 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, 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 Applicable Data Protection Laws. These include:

- The IGC does not record personal information of an end user against the services, using network identifiers for individual services instead.
- Encryption is used both in transit and at rest using methods such as Transport Layer Security (TLS), for example, Hypertext Transfer Protocol Secure (HTTPS) and Secure File Transfer Protocol (SFTP), Internet Protocol Security (IPsec), Virtual Private Networks (VPNs) and hardware encryption.
- Data at rest is protected by implementing multiple physical and logical controls. These controls reduce the risk of unauthorised access or mishandling of information and Personal Data, which might affect its confidentiality, availability, and integrity. Data at rest in the centralised storage is protected with hardware encryption or software encryption.
- Where local storage solutions are not encrypted, the confidentiality of the data is protected by physical access controls and routines for handling secure disposal of removable media. Local storage is only used for storage of unconsolidated data for shorter time frames. Backups are stored within the production platform in the redundant site and are encrypted.
- IGC components are constantly monitored by Subprocessor (1)'s Security Incident Response Team, ensuring that all components are updated against vulnerabilities and latest remedial actions.

- IGC uses enforced password change, complex password security controls, locking of user accounts, session time-outs, role-based access and user log on history by default to prevent unauthorized access. Operators can further enable optional controls to further increase security such as CAPTCHA code, two-step authentication, and password aging.
- All IGC equipment is hosted in physically secured tier 3 data centres provided by third parties. The multi-tenant IGC data centres are ISO 27001 Information Security Management and ISO 22301 Business Continuity Management certified. Strict physical access controls to the data centres are followed by subsequent logical security controls, including access management, controlled authentication, the encryption of databases, disk encryption, firewalls, network segmentation, data retention, the secure disposal of data and specific security manual routines.
- For public cloud resources used, specific controls, such as access control management, cryptography, and data retention policies are implemented.
- Subprocessor (1) complies with ISO/IEC 27001:2013.
- Users can directly request access to, correction or erasure of, their Personal Data via the self-service portal.

List of Subprocessors

Telstra has engaged the following Subprocessors:

1. Aeris Communications, Inc. for Transfer (a) Customer registration details; Transfer (b): Portal configuration and activity; Transfer (c): Request via the Application Programming Interface (API)
2. CSG International Australia Pty Ltd for Transfer (a) 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.