Description of Data Processing – GMNS with Highlight

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.

Categories of Personal Data

Transfer (a): User account and log details: Generated through the Authorised User's activity on the platform, including first/ last name, email address, role/ job title and network device information, which might include IP addresses.

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

The parties acknowledge that since the data processing for this Service is limited to that processed within the platform environment, Telstra does not Process any Personal Data comprised in the contents of communications data sent and received over Customer's network and devices, 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) User account and log details	Store and hosting by the Subprocessor listed in this document. Access by this Subprocessor and Telstra personnel and/or affiliates for account support, and customisation	Continuous storage and hosting; access on an as need basis upon request	Deleted from the active databases within 90 days of termination of the agreement unless storage required by applicable law. Partial data remains stored in back-ups for up to 12 months.

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 Authorised User Personal Data. **Identification:** Telstra users are granted a unique ID before being granted access to any systems containing 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 Authorised User Personal Data required to perform their role. This includes record-keeping of authorised system users with access to Authorised User 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 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 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

Standard	Practices
	for all weak, non-approved algorithms. Access to encryption keys is recorded and audited at least annually.
Data Protection	**Information classification:** Authorised User Personal Data is classified as such to meet applicable requirements under data protection laws. This enables Telstra to remove 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 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 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 Authorised User Personal Data. Logs for systems that store, process, or transmit 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 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.

Standard	Practices
Supplier Management	**Due diligence:** Telstra requires that a partner security assessment is undertaken for suppliers that have the potential to access 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 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 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/privacypolicy.

In addition to the supplier management controls detailed above, Telstra also employs specific technical and organisational measures to ensure Subprocessors are able to provide assistance in meeting obligations under relevant data protection laws. The Subprocessor involved under Transfer (a) utilises encryption in transit and during storage where ISO 27001 standards are applied. User identification and authorisation controls are applied via Secure Sign-On via a user portal, with users being required to re-validate logins every 3 months. There is a role-based access control with cascading privileges to provide a granular control of user and administrator access in accordance with "least privilege" and "need to know" principles. Additionally, login information which is not actively used for a given period is first suspended and after a confirmation period, deleted to ensure data minimisation.

List of Subprocessors

Telstra has engaged the following Subprocessors:

- Highlight (SLM) Limited for Transfer (a): User account and log 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.