Description of data processing – Managed SSE (Palo Alto)

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) The accounts of persons connecting to your network or systems, or details about persons attempting to connect or gain access to your network or systems ("**Network Users**").

Categories of Personal Data

Transfer (a): **Customer portal information:** In order to create the accounts and provide access to the service portal we may process Authorised User details via your identity management system. These would typically include Authorised User's first name and surname, user ID, title, office address and/or phone numbers, and email;

Transfer (b): **Portal activity**: It captures details about user activity such as login date, details of changes made by individual users, detail of the change and the relevant date; and/or,

Transfer (c): **Information processed as part of the Service**: This information includes hostnames, MAC addresses, IP addresses, email addresses, and user names of Network Users. The proxy logs may contain records of Network Users' email, indicate applications used or web browsing requests made through the Customer's proxy server. Where Authorized Users download the GlobalProtect App, individual device information might be collected, including IMSI, IMEI, HostID data, access location, and/or IP address details.

In extremely limited and rare circumstances, proxy log records may include user browsing requests sent via the Customer's server that could indirectly suggest sensitive information or special categories of Personal Data about an Authorized User and/or a Network User. In these circumstances, Telstra uses a strict, role-based access model, which limits access to system features and data using a 'need to know' and least privileged access model. All role-based access requires approval by appropriate delegates. All access to relevant data and systems is audited and reviewed. Additionally, Customers can enable and disable sharing of log types with Telstra and the Subprocessor listed in this document in accordance with their policies and limit log forwarding to third parties via role based access controls.

While it is highly unlikely that Telstra personnel would, or could, view any Special Categories of Personal Data in logs, Telstra is committed to further protecting this data by implementing additional controls such as: (a) including information in guidelines that the logs are only 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): Customer registration details; Transfer (b): Portal activity; Transfer (c): Information processed as part of the Service	Storage by the Subprocessor listed in this document, and access by Telstra and such Subprocessor to ensure compliance with Customer's security policies and for assurance purposes	Storage on a continuous basis and access on an as needed basis	Determined by Customers based on their retention schedule or storage size. Upon termination of the Service, Data remains active in the systems for 30 days, and is purged from the system within additional 30 days. Purge of backup data occurs within additional 150 days.

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 Network User and Authorised User Personal Data.

Standard	Practices
	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. **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

Standard	Practices
	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 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 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 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.

Standard	Practices
	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 organizational 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, the Subprocessors listed in this document also employs specific technical and organisational measures to ensure that they are able to provide assistance in meeting obligations under relevant Applicable Data Protection Laws. These include:

- Telstra uses Multi Factor Authentication to access the portal and all access is logged.
- Logs are encrypted in transit to a data center of Customer's choice, and logs hosted in GCP are encrypted at rest.
- The data centers are secured and protected with state-of-the-art physical and network security, the latter provided by industry leading technology. The Subprocesor has obtained SOC 2 Type II certification and the service is hosted in data centers certified as SOC 2 Type II.
- Rigorous technical and organisational security controls are applied.
- Processing of raw logs in automated.
- Customers can choose a specific regional data center for storage of their logs. Logs and information forwarded to the European data center will remain in the European Union.
- Customers can enable or disable sharing of log types in accordance with their policies and they can also control access to the firewall logs.
- Internal and external vulnerability scans are run quarterly and a qualified third party is engaged to conduct the application security assessments.
- Data is physically or logically separated, and Personal Data and end user data is segregated from its other customer's data.

List of Subprocessors

Telstra has engaged the following Subprocessors:

- Palo Alto Networks (Netherlands) B.V. for Transfer (a): Customer registration details; Transfer (b): Portal activity; Transfer (c): Information processed as part of the Service

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.