Data Protection Addendum

1. Interpretation

1.1 This Data Protection Addendum ("**DPA**") forms part of, and is incorporated into the Services Agreement or Service Order Form entered into between Customer, on behalf of itself and its Authorised Affiliates, and Telstra for the provision of the Services referred to in this Addendum (the "Services").

1.2 Capitalised terms that are not defined in this DPA have the meaning specified in the GDPR or the UK GDPR (as the context requires).

1.3 The Services Agreement and each Service Order Form agreed between you and us shall remain in full force and effect; provided that this DPA shall supersede and replace any other data protection agreement, addendum or clauses that the parties or their Affiliates may have previously entered into that would otherwise apply to subject matter of this DPA.

1.4 This DPA contains the mandatory clauses required by Article 28 of the GDPR and equivalent provisions contained in the UK GDPR. These provisions shall only apply in the circumstances where provision of the Services, including the associated Processing of your Personal Data, is covered by such provisions.

2. Processing of your Personal Data

Our Processing of Personal Data

2.1 We shall not Process your Personal Data other than on your documented instructions unless Processing is required by Applicable Laws, in which case we shall to the extent permitted by such law inform you of that legal requirement before the relevant Processing of your Personal Data.

2.2 You instruct us (and authorise us to instruct each Subprocessor) to:

2.2.1 Process your Personal Data; and

2.2.2 in particular, transfer your Personal Data to any third country or territory,

in connection with the provision of goods and services to you in accordance with the Services Agreement and each Service Order Form and this DPA, including the SCC Annexes.

2.3 This DPA incorporates the Standard Contractual Clauses (**SCCs**) approved the purposes of allowing you and us to lawfully transfer personal data in accordance with Article 46 of the GDPR and its equivalent terms in the UK GDPR.

2.4 In relation to Personal Data that we and our Subprocessors (each, a Contracted Processor) may Process in the course of supplying goods or performing Services for you, each Contracted Processor will comply with the SCCs, and will Process your Personal Data as described in the details contained in the SCC Annexes.

3. Our Personnel

3.1 We shall ensure that all employees of any Contracted Processor who have access to your Personal Data are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 We shall implement and maintain, and shall ensure that each Subprocessor implements and maintains, in relation to the Service the technical and organisational measures set out in the SCC Annexes with respect to all Processing of your Personal Data pursuant hereto by Contracted Processors.

4.2 You represent, undertake and warrant that at all times all Personal Data Processed by the Contracted Processors that is provided by you, or on your behalf has been and shall be collected and processed by you in accordance with all Applicable Laws and without limitation to the foregoing you shall take all steps necessary, including without limitation providing appropriate fair collection notices and ensuring that at all times there is a lawful basis for Contracted Processors to process such Personal Data, to ensure that the Processing of such Personal Data by Contracted Processors is compliant with Applicable Laws. You shall indemnify and hold harmless each Contracted Processor against all claims (including any claims by any Supervisory Authority), losses, fines and sanctions of any kind arising from, or in connection with, any breach of section 4.2.

4.3 You may implement additional technical and organisational measures ("**Customer Security Measures**") from time to time for the purpose of complying with your obligations under the GDPR and the UK GDPR in respect of the Service, provided that:

4.3.1 at all times you will ensure that all Customer Security Measures are compatible with our technical and organisational measures described in the SCC Annexes; and

4.3.2 no Contracted Processor shall be required to change any of the technical or organisational measures set out in the SCC Annexes, or incur any costs of implementing or supporting any Customer Security Measures.

5. Subprocessing

5.1 You authorise us to engage the Subprocessors specified in the SCC Annexes for the specified purposes described in the SCC Annexes and authorise us, to appoint further

Subprocessors in accordance with this section 5 and subject to the requirements of the SCCs.

5.2 We shall give you at least fourteen (14) days' prior written notice of the appointment of any new Subprocessor or changes to any Subprocessor's Processing arrangements, including necessary details of the Processing to be undertaken by the Subprocessor.

5.3 If, within fourteen (14) calendar days of our notice, you notify us in writing of any objections (on reasonable grounds) to the proposed appointment, we shall at our option:

5.3.1 not appoint (or disclose any of your Personal Data to) that proposed Subprocessor until it has taken reasonable steps to address the objections raised by you; or

5.3.2 notify you that you may terminate the Service without incurring any early termination costs, notwithstanding any term of the Services Agreement or any Service Order Form to the contrary.

5.3.3 For the avoidance of doubt, your right to terminate an affected Service under section 5.3.2 shall not extend to non-impacted services and is otherwise without prejudice to the Parties' rights and obligations in relation to any terminated Service up to, and including the date of termination.

5.4 With respect to each Subprocessor, we shall ensure that the Subprocessor's Processing is governed by a written contract including terms which offer at least the same level of protection for your Personal Data as those set out in this DPA.

6. Data Subject Rights

6.1 We shall:

6.1.1 promptly notify you if any Contracted Processor receives a request from a Data Subject under any EU or UK Data Protection Law in respect of your Personal Data; and

6.1.2 ensure that we, or any Subprocessor, do not respond to that request except on your documented instructions or as required by Applicable Laws, in which case we shall to the extent permitted by Applicable Laws inform you of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

We shall notify you without undue delay upon us or any Subprocessor becoming aware of a Personal Data Breach affecting your Personal Data, providing you with information (as and when available) to assist you to meet any obligations to report or inform affected Data Subjects of the Personal Data Breach under Applicable Data Protection Laws.

8. Data Protection Impact Assessment and Prior Consultation

We shall provide reasonable information and assistance to you in relation to any data protection impact assessments you need to complete in order to comply with your obligations under UK or EU Data Protection Laws in relation to our services, to the extent you do not have access to relevant information already and to the extent that such information is available to us.

9. Deletion or return of your Personal Data

9.1 Subject to sections 9.2 and 9.3 and to the requirements of any applicable exit plan, you instruct us to, after the date of cessation of any Services involving the Processing of your Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of your Personal Data.

9.2 You acknowledge and agree that you will be responsible for making a copy of or exporting, before the Cessation Date (or any later date as specifically set out in the applicable Service Schedule or Service Order Form), any of your Personal Data which you wish to retain.

9.3 Each Contracted Processor may retain your Personal Data to the extent required by local laws applicable to such Contracted Processor and only to the extent and for such period as required by such laws and always provided that the Contracted Processor shall ensure the confidentiality of such Personal Data and shall ensure that your Personal Data is only Processed as necessary for the purpose(s) specified by such laws and for no other purpose.

10. Audit rights

10.1 Subject to sections 10.2 to 10.3, we shall make available to you on request all information reasonably necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, of the processing activities covered by this DPA, in accordance with the relevant modules of the SCCs.

10.2 You shall give us reasonable notice of any audit or inspection to be conducted under section 10.1. We may object in writing to an auditor appointed by you to conduct any audit under section 10.1 if the auditor is, in our reasonable opinion, not suitably qualified or independent, a competitor of ours, or otherwise manifestly unsuitable. Any such objection by us will require you to appoint another auditor.

10.3 If we request you to do so, you must procure that any auditor appointed by you other than you or your employee(s) signs suitable confidentiality undertakings in respect of our Confidential Information to our reasonable satisfaction prior to undertaking any audit in accordance with this section 10.

10.4 You shall make (and ensure that each appointed auditor makes) all necessary efforts to avoid causing any damage, injury or disruption to any Contracted Processor's

premises, equipment, personnel and business in the course of such an audit or inspection. We need not give access to our premises for the purposes of such an audit or inspection:

10.4.1 to any individual unless he or she produces reasonable evidence of identity and authority;

10.4.2 outside normal business hours at those premises, unless the audit or inspection is required to be carried out on an emergency basis by a Supervisory Authority; or

10.4.3 for the purposes of more than one audit or inspection, in any calendar year, except for any additional audits or inspections which you are required or requested to be carried out pursuant to Applicable Data Protection Laws, by order or direction of a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Applicable Laws in any country or territory.

11. General Terms

Order of precedence

11.1 Notwithstanding any other order of precedence clause in the Services Agreement Terms, any Service Schedule or Service Order Form, in relation to Processing of Personal Data, in the event of any conflict or inconsistency the following descending order of precedence shall apply:

11.1.1 The SCCs (including the SCC Annexes);

11.1.2 the terms of this DPA;

11.1.3 the terms of the Service Order Form;

11.1.4 the terms of each Service Schedule; and

11.1.5 to the extent applicable, the terms of any Services Agreement.

Governing Law & Supervisory Authority

11.2 Notwithstanding any other governing law clause in the Services Agreement, any Service Schedule or Service Order Form, in respect of any Personal Data exported from the EU and for the purposes of clauses 17 and 18 of the SCCs, the Processing of such Personal Data and any applicable data transfers are governed by the laws of Ireland, and the parties submit to the non-exclusive jurisdiction of the Irish courts and courts entitled to hear appeals from them.

11.3 Notwithstanding any other governing law clause in the Services Agreement, any Service Schedule or Service Order Form, in respect of any Personal Data exported from the United Kingdom, the Processing of such Personal Data and any applicable data transfers are governed by the Courts of England and Wales and the parties submit

to the non-exclusive jurisdiction of the English courts and courts entitled to hear appeals from them.

11.4 For the avoidance of doubt, in respect of any Personal Data exported from the EU, the parties acknowledge (and this DPA does not limit or seek to modify) the right of any Data Subject whose Personal Data is subject of this DPA to bring legal proceedings against either party in the Data Subject's country of habitual residence, if they are resident in a Member State.

Changes in Applicable Laws

11.5 If any variation is required to this DPA as a result of a change in Applicable Data Protection Laws, including any replacement of or variation to the Standard Contractual Clauses, then either party may provide written notice to the other party of that change in law. The parties shall discuss the change in Applicable Data Protection Laws and negotiate in good faith with a view to agreeing any necessary variations to this DPA, including the Standard Contractual Clauses, to address such changes.

Severance

11.6 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Costs

11.7 You shall reimburse us for all costs (including internal and third party costs) which are reasonably and properly incurred by us in the performance of our obligations under sections 6 (Data Subject Rights); 7 (Personal Data Breach); 8 (Data Protection Impact Assessment and Prior Consultation) and 10 (Audit rights) of this DPA. We shall charge for internal resources at our current professional day rates as set by us from time to time.

Notices

11.8 Any notice required to be given under this DPA must be sent by email to, in the case of notices to Customer, the contact person specified in the Services Agreement (if applicable), or the relevant Service Order Form and, in the case of notices to Telstra to privacy@online.telstra.com.au.

12. Definitions

12.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

12.1.1 "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for

purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity;

12.1.2 "**Applicable Data Protection Laws**" EU Data Protection Laws, UK Data Protection Laws directly applicable to any personal data processed pursuant to this Addendum;

12.1.3 "**Applicable Laws**" means in the case of Personal Data that is subject to the UK GDPDR, any UK law, and in the case of Personal Data that is subject to the GDPR, any European Union or Member State laws.

12.1.4 **"Authorised Affiliate**" means each Customer Affiliate(s) which:

12.1.4.1 is a Controller of Personal Data Processed by Telstra pursuant to this DPA, which data is subject to EU or UK Data Protection Laws; and

12.1.4.2 is permitted to use the Services pursuant to the Services Agreement or a Service Order Form between Customer and Telstra, but which has not signed its own Services Agreement or Service Order Form with Telstra and is not a "Customer" as defined in this DPA;

12.1.5 "**Contracted Processor**" means us or a Subprocessor;

12.1.6 "**Confidential Information**" has the meaning given in the Services Agreement;

12.1.7 **"Customer" or "you"** means the customer and its Authorised Affiliates described in the Services Agreement and any Service Order Form for the Services, including, in the case of any obligations hereunder, any Authorised Affiliate;

12.1.8 **"EEA" means the European Economic Area;**

12.1.9 "**EU Data Protection Laws**" means the Data Protection Directive (95/46/EC) if applicable, the GDPR and the ePrivacy Directive (2002/58/EC), including implementing or supplementing laws, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time;

12.1.10 "**GDPR**" means EU General Data Protection Regulation (2016/679);

12.1.11 "**SCC Annexes**" mean the Annexes to the SCCs contained in the Appendix to this DPA.

12.1.12 "**Service**" means the Service described in the Service Schedules or any Service Order Form supplied by us or our Affiliates that involves the Processing of Personal Data as described in the SCC Annexes;

12.1.13 "**Services Agreement**" means our Global Business Services Agreement or other services agreement that we agree with you in writing for the provision of Services;

12.1.14 "**Service Order Form**" means our standard Service Order Form for Services, or any other order form that we agree with you in writing that incorporates the provisions of this DPA;

12.1.15 "**Service Schedules**" mean the Service Schedules to the Services Agreement;

12.1.16 "**Standard Contractual Clauses or SCCs" means:**

12.1.16.1 In the case of Personal Data exported from the EEA: the contractual clauses located at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN, which for avoidance of doubt shall include all Module Two clauses included therein, in each case, as may be amended supplemented or replaced by the European Commission from time to time, and incorporating as Annexes the information contained in the Appendix to this DPA.

12.1.16.2 in the case of Personal Data exported from the United Kingdom, the contractual clauses set forth in clause 12.1.16.1 above, as supplemented and amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "IDTA") located at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf. Table 1 to the IDTA shall be deemed to include the information at the beginning of this Agreement. Table 2 to the IDTA shall refer to the contractual clauses set forth in clause 12.1.16.1 above. Table 3 of the IDTA shall refer to the information contained in the applicable Annexes contained in the Appendix to this DPA. For purposes of Table 4 to the IDTA, the parties agree that Importer may end this Addendum as set out in Section 19 of the IDTA; and any amendment or replacement of these terms (as applicable) published from time to time;

12.1.17 "**Subprocessor**" means any person (including any third party and any Telstra Affiliate, but excluding us and our personnel) appointed by or on behalf of us to Process Personal Data on behalf of you in connection with this DPA;

12.1.18 **"Telstra" or "we"** means the Telstra entity set forth in the Services Agreement or the applicable Service Order Form;

12.1.19 "**Telstra Affiliates**" means each Affiliate of Telstra, referred to in the SCC Annexes;

12.1.20 "**UK Data Protection Laws**" means the Data Protection Act 2018 (incorporating the UK GDPR) and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and the laws implementing or supplementing them;

12.1.21 “**UK GDPR**” means the UK General Data Protection Regulation as defined in the Data Protection Act 2018 (UK); and

12.1.22 "**your Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of you pursuant to this DPA.

12.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", “**Personal Data Breach**”, “**Processor,** "**Processing**” and "**Supervisory Authority**" and other defined terms contained in the GDPR or UK GDPR shall in the context of processing to which EU Data Protection Laws apply, have the same meaning as in the GDPR and in the context of processing to which UK Data Protection Laws apply, shall have the same meaning as in the UK GDPR.

APPENDIX

Annexes I, II and III (1, 2 and 3) to the SCCs

ANNEX I

A. LIST OF PARTIES

Data Exporter: Customer. Customer's address and other relevant details are identified in the Service Order Form. Customer is the Controller. Customer is using the Services as further described in the Service Order Form which may involve the data transfers described below.

Data Importer: Telstra and its Affiliates. With respect to Telstra, its address and other relevant details are identified in Annex III. Telstra is providing the Services as described in the Service Order Form which may involve Telstra's undertaking the data transfers described below as a Processor. Depending on the Services, Telstra may use Affiliates to assist with Subprocessing. These Affiliates and their addresses are listed in Annex III.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is transferred

(i) The accounts and details 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**"); and/or

(ii) Users you authorise to use or assist with the Service and any employees, agents, advisors, and other authorised representatives of the customer nominated for those purposes ("**Authorised Users**").

Categories of Personal Data transferred

Transfer (a): **Information processed as part of the Service:** Hostnames, MAC addresses, IP addresses, email addresses, and user names of Network Users, may be included in some of the log data the customer sends to Telstra as part of the Service. Other Personal Data may be included in proxy logs, which Telstra may monitor upon your request. These proxy logs may contain records of Network Users' email or web browsing requests made through the customer's proxy server.

Transfer (b): **Information processed to facilitate the Service:** You may provide Telstra with various pieces of contextual information about your network and Network Users that Telstra processes to provide the Service. This may include a list of critical user accounts, the names and job titles of the users associated with those accounts, and a list of critical administrator accounts and critical assets.

Transfer (c): **Customer contact information:** A contact list of Authorised Users, which Telstra processes for escalations and technical assistance, and to provide Authorised Users with access to a service portal. This contact list may include first

and last names, email addresses, office and mobile phone numbers, and the contact's title.

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 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. No on-forwarding of data or transfer to third-parties is permitted except in circumstances where the data originated from the requester and is subject to their ownership and accountabilities as the originators of the data.

While it is highly unlikely that Telstra personnel would, or could, view any Special Categories of Personal Data in logs, Telstra is commited 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): Information processed as part of the Service; Transfer (b): Information processed to faciliate the Service; Transfer (c): Customer contact information	Storage and access by Telstra affiliates and personnel to monitor and detect potential cyber security incidents, and to enable the protection of customer data and systems from unauthorised access by cyber attackers.	Storage and monitoring on a continuous basis	Relevant data is automatically destroyed in accordance with a retention period as agreed with each customer, up to a maximum of 7 years. Data can also be manually destroyed on the customer's request.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the Irish Data Protection Commission where the EU GDPR applies and the United Kingdom Information Commissioner's Office where the UK GDPR applies.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Telstra protects all third country transfers of Personal Data, undertaken by Telstra personnel or affiliates as detailed in Annex III, 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. **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.

Standard	Practices
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 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

Standard	Practices
	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. **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.

ANNEX III

LIST OF SUB-PROCESSORS

The Controller has authorised the use of the following sub-processors, per Clause 9(a) Option 1:

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

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is transferred

(iii) The accounts and details 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**"); and/or

(iv) Users you authorise to use or assist with the Service and any employees, agents, advisors, and other authorised representatives of the customer nominated for those purposes ("**Authorised Users**").

Categories of Personal Data transferred

Transfer (d): **Information processed as part of the Service:** Hostnames, MAC addresses, IP addresses, email addresses, and user names of Network Users, may be included in some of the log data the customer sends to Telstra as part of the Service. Other Personal Data may be included in proxy logs, which Telstra may monitor upon your request. These proxy logs may contain records of Network Users' email or web browsing requests made through the customer's proxy server.

Transfer (e): **Information processed to facilitate the Service:** You may provide Telstra with various pieces of contextual information about your network and Network Users that Telstra processes to provide the Service. This may include a list of critical user accounts, the names and job titles of the users associated with those accounts, and a list of critical administrator accounts and critical assets.

Transfer (f): **Customer contact information:** A contact list of Authorised Users, which Telstra processes for escalations and technical assistance, and to provide Authorised Users with access to a service portal. This contact list may include first and last names, email addresses, office and mobile phone numbers, and the contact's title.

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 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. No on-forwarding of data or transfer to third-parties is permitted except in circumstances where the data originated from the requester and is subject to their ownership and accountabilities as the originators of the data.

While it is highly unlikely that Telstra personnel would, or could, view any Special Categories of Personal Data in logs, Telstra is commited 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): Information processed as part of the Service; Transfer (b): Information processed to faciliate the Service; Transfer (c): Customer contact information	Storage and access by Telstra affiliates and personnel to monitor and detect potential cyber security incidents, and to enable the protection of customer data and systems from unauthorised access by cyber attackers.	Storage and monitoring on a continuous basis	Relevant data is automatically destroyed in accordance with a retention period as agreed with each customer, up to a maximum of 7 years. Data can also be manually destroyed on the customer's request.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the Irish Data Protection Commission.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Telstra protects all third country transfers of Personal Data, undertaken by Telstra personnel or affiliates as detailed in Annex III, 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. **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.

Standard	Practices
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 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

Standard	Practices
	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. **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.

In addition to the security standards detailed above, Telstra also employs the following specific security controls to protect transfers:

- For Transfer (a): Information processed as part of the Service, IP addresses are pseudonymised by restricting them to country-level geographic location/s, so that they not sufficient to identify a person or a location.
- Telstra employs 'hardening' of configurations, along with regular patching and vulnerability scans, so that systems holding all transferred data, as outlined in Annex I, meet security requirements.
- Extensive and resilient business continuity and disaster recovery systems to help ensure the continuity of operations and access to all transferred data listed in Annex I.

- Annual re-certification of systems that hold all transferred data listed in Annex I, which includes an extensive audit of security controls and independent annual security penetration testing to validate the effectiveness of controls.

ANNEX III

LIST OF SUB-PROCESSORS

Per Clause 9(a) Option 1, the Controller has authorised the use of Telstra affiliates listed here, as updated from time to time.