Data Protection Addendum

This Data Protection Addendum ("**Addendum**") forms part of the master agreement ("**Agreement**") between: (i) **Telstra Limited, Telstra GmbH or Telstra SARL** (as applicable, "**we**", "**us**", "**our**" or "**Telstra**") and (ii) **you** (as defined in the Agreement).

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties agree that the terms and conditions set out below shall be incorporated as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Processing of your Personal Data

1.1 We shall not Process your Personal Data other than on your documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, 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.

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

1.2.1 Process your Personal Data; and

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

as reasonably necessary to the provision of the Services and consistent with the Agreement.

1.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of your Personal Data as required by Article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). You may make reasonable amendments to Annex 1 by written notice to us from time to time as you reasonably consider necessary to meet those requirements. As between the parties, nothing in Annex 1 (including as amended pursuant to this section 1.3) confers any right or imposes any obligation on either party.

2. Our Personnel

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.

3. Security

3.1 During the Term, we shall implement and maintain, and shall ensure that each Contracted Processor implements and maintains the technical and organisational measures set out in Appendix 2 to the Standard Contractual Clauses with respect to all processing of your Personal Data by Contracted Processors. You may implement additional reasonable measures ("**Security Measures**") from time to time always provided that (a) such Security Measures are compatible with the measures set out in Appendix 2 to the Standard Contractual Clauses as determined by us acting reasonably and (b) neither us nor any Contracted Processor shall be required to change any of the measures set out in Appendix 2 to the Standard Contractual Clauses or to incur any costs implementing or supporting the implementation of your Security Measures.

3.2 You represent, undertake and warrant that:

3.2.1 on the date of the Agreement and during the Term of the Agreement, those technical and organizational measures set out in Appendix 2 to the Standard Contractual Clauses together with any Security Measures which you may implement from time to time in accordance with section 3.1 above, collectively meet the requirements set out in Data Protection Laws; and

3.2.2 on the date of the Agreement and during the Term of the Agreement, all your Personal Data Processed by the Contracted Processors has been and shall be collected and processed by you in accordance with all applicable Data Protection Laws and without limitation to the foregoing you shall take all steps necessary, including without limitation providing appropriate fair collection notices and ensuring that there is a lawful basis for Contracted Processors to process your Personal Data, to ensure that the processing of your Personal Data by Contracted Processors in accordance with the Agreement is in accordance with all Data Protection Laws.

3.3 You shall indemnify and hold harmless us and each Contracted Processor authorized by you in accordance with this Addendum against all losses, fines and sanctions howsoever arising from any claim by a third party (including any Supervisory Authority) arising from any breach of section 3.2.

4. Subprocessing

4.1 You authorise us to appoint (and permit each Subprocessor appointed in accordance with this section 4 to appoint) Subprocessors in accordance with this section 4 and any restrictions in the Agreement.

4.2 We may continue to use those Subprocessors already engaged by us as at the date of this Addendum, subject to us, in each case as soon as practicable, meeting the obligations set out in section 4.4.

4.3 We shall give you prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 30 calendar days of receipt of that notice, you notify us in writing of any objections (on reasonable grounds) to the proposed appointment, we shall 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 and provided you with a reasonable written explanation of the steps taken.

4.4 With respect to each Subprocessor, we shall:

4.4.1 before the Subprocessor first Processes your Personal Data (or, where relevant, in accordance with section 4.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for your Personal Data required by the Agreement;

4.4.2 ensure that the arrangement between us (or the relevant intermediate Subprocessor) and the Subprocessor 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 Addendum; and

4.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between us (or the relevant intermediate Subprocessor) and the Subprocessor, or before the Subprocessor first Processes your Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with you or we enter into the Standard Contract Contractual Clauses on your behalf and you hereby authorise us to do so.

5. Data Subject Rights

5.1 We shall:

5.1.1 promptly notify you if we, or any Contracted Processor, receive a request from a Data Subject under any Data Protection Law in respect of your Personal Data; and

5.1.2 ensure that we, or any Contracted Processor, do not respond to that request except on the documented instructions of you or as required by Applicable Laws to which the Contracted Processor is subject, 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.

6. 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.

7. Data Protection Impact Assessment and Prior Consultation

We shall provide reasonable assistance to you with any data protection impact assessments, and prior consultations with Supervisory Authorities, which you reasonably consider to be required of any of your Group Companies by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of your Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

8. Deletion or return of your Personal Data

8.1 Subject to sections 8.1 and 8.3 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.

8.2 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), any of your Personal Data which you wish to retain.

8.3 Each Contracted Processor may retain your Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by such laws and always provided that we 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 in such laws requiring its storage and for no other purpose.

9. Audit rights

9.1 Subject to sections 9.2 to 9.3, we shall make available to you on request all information necessary to demonstrate compliance with this Addendum, and shall

allow for and contribute to audits, including inspections, by an auditor appointed by you in relation to the Processing of your Personal Data by the Contracted Processors.

9.2 You shall give us reasonable notice of any audit or inspection to be conducted under section 9.1. We may object in writing to an auditor appointed by you to conduct any audit under section 9.1 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.

9.3 You shall make (and ensure that each appointed auditor makes) reasonable endeavours to avoid causing any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

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

9.3.2 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

9.3.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which you are required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory.

10. Restricted Transfers

10.1 Subject to section 10.3, you (as "data exporter") and us acting on our own behalf and as agent for each Telstra Group Company (each as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from you to us or the relevant Telstra Group Company.

10.2 The Standard Contractual Clauses shall come into effect under section 10.1 on the later of:

10.2.1 the data exporter becoming a party to them;

10.2.2 the data importer becoming a party to them; and

10.2.3 commencement of the relevant Restricted Transfer.

10.3 Section 10.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from data subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

10.4 We warrant that we are and will at all relevant times remain duly and effectively authorised to act on behalf of each relevant Telstra Group Company for the purposes of section 10.1.

11. General Terms

Order of precedence

11.1 In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

11.2 Subject to section 11.1, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws

11.3 If any variation is required to this Addendum as a result of a change in Data Protection Law, 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 Data Protection Law and negotiate in good faith with a view to agreeing any necessary variations to this Addendum, including the Standard Contractual Clauses, to address such changes.

Severance

11.4 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum 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

11.5 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 5 (Data Subject Rights); 6 (Personal Data Breach); 7 (Data Protection Impact Assessment and Prior Consultation) and 9 (Audit rights) of this Addendum. We shall charge for internal resources at our current professional day rates as set by us from time to time.

Indemnity

11.6 You shall indemnify and hold harmless us and each Contracted Processor authorized by you in accordance with this Addendum against all losses, fines and sanctions howsoever arising from any breach of this Addendum by you.

11.7 You acknowledge and agree that any losses, fines and sanctions suffered by a Subprocessor (authorized by you in accordance with this Addendum) pursuant to

clauses 3.3 and 11.6 of this Addendum shall be recoverable by us as if such losses, fines and sanctions had been suffered by us ourselves.

12. Definitions

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

12.1.1 "**Applicable Laws**" means any UK, European Union or Member State laws and, to the extent applicable, the laws of any other country;

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

12.1.3 "**Data Protection Laws**" means EU Data Protection Laws, UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

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

12.1.5 "**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,;

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

12.1.7 "**Restricted Transfer**" means:

12.1.7.1 a transfer of your Personal Data from you to a Contracted Processor; or

12.1.7.2 an onward transfer of your Personal Data from a Contracted Processor to (or between two establishments of) a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 4.4.3 or 10 above;

12.1.8 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised third-party access to, personal data transmitted, stored or otherwise processed;

12.1.9 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section 11.3 and any amendment or replacement contractual clauses that are approved in accordance with applicable Data Protection Laws;

12.1.10 "**Subprocessor**" means any person (including any third party and any Telstra Group Company, but excluding any employee of ours or any of our sub-contractors) appointed by or on behalf of us to Process Personal Data on behalf of you in connection with the Agreement;

12.1.11 "**UK Data Protection Laws**" means the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and the laws implementing or supplementing these legislation; and

12.1.12 "**your Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of you pursuant to or in connection with the Agreement.

12.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

ANNEX 1: DETAILS OF PROCESSING OF YOUR PERSONAL DATA

This Annex 1 includes certain details of the Processing of your Personal Data.

Subject matter and duration of the Processing of your Personal Data

The subject matter and duration of the Processing of your Personal Data are set out in the Agreement and this Addendum.

The nature and purpose of the Processing of your Personal Data

The nature and purpose of the Processing of your Personal Data are set out in the Agreement and this Addendum.

The types of your Personal Data to be Processed

(i) name (forename, middle name(s) and surname), birth name, maiden name or any additional names, address, title, preferred salutation;

(ii) business contact information (company, telephone number, email address, business address), personal contact information (company, telephone number, email address, address), social media username or alias and other contact information;

(iii) professional life data including occupation, employer, employment status, income, and other occupation or income related data;

(iv) personal life data including marital status, lifestyle, hobbies and interests, and other background data and relationship management information;

(v) unique account or customer numbers, or other of your internal identifiers;

(vi) bank account numbers, names and transaction descriptions other transaction details;

(vii) your employee numbers or other of your internal identifiers and names, job titles and email addresses;

(viii) instant message or live chat logs;

(ix) meeting, telephone or attendance notes, emails, letters or other data relating to communications, calls and meetings;

(x) on-going monitoring data in connection with compliance and/or fraud prevention;

(xi) IP address, browser generated information, device information, geo-location markers and other digital identifiers used for tracking, profiling or location purposes;

(xii) end user usage information of your applications; and

(xiii) other metadata relating to the use of your systems and applications.

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.

The types of special categories of your Personal Data to be Processed

No special categories of your Personal Data are Processed under the Agreement or this Addendum.

The categories of Data Subject to whom your Personal Data relates

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

(ii) suppliers, subcontractors, vendors and business partners of you ("**Third Parties**") and employees, agents, advisors, and other authorised representatives of Third Parties;

(iii) users authorised by you to use the Service ("**Authorised Users**") and any employees, agents, advisors, and other authorised representatives of Authorised Users;

(iv) visitors to your websites and persons connecting, or attempting to connect or gain access to your network or systems;

(v) current, prospective and former employees, contractors, agents, officers, directors and other representatives of you ("**Staff**");

(vi) relatives, dependents and beneficiaries of Staff;

(vii) professional advisors and consultants to you.

Your obligations and rights

Your obligations and rights are set out in the Agreement and this Addendum.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

[*These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law*[1] *(otherwise).*]

[*If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".*]

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection [*This opening recital is deleted if these Clauses are not governed by the law of a member state of the EEA.*]

[*The gaps below are populated with your details:*]

Name of the data exporting organisation:

Address:

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organisation

……
(the data **exporter**)

And

[*The gaps below are populated with details of us or the relevant Telstra Group Company:*]

Name of the data importing organisation:

Address:

Tel.: _____; fax: _____; e-mail:_____

Other information needed to identify the organisation:

……
(the data **importer**)

[1] The standard clauses are of course approved by the European Commission and not by any equivalent authority. The reference here is intended to capture possible deemed approval of the same standard clauses by an equivalent UK authority on or after Brexit (or, in theory, an equivalent authority in another departing Member State in the future).

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; [*If these Clauses are not governed by the law of a Member State, the words "and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC" are deleted.*]

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified

to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; [*If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.*]

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract

contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
[*Populated with details of, and deemed signed on behalf of you, as the data exporter:*]
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

On behalf of the data importer:
[*Populated with details of, and deemed signed on behalf of us or the relevant Telstra Group Company, as the data importer:*]
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter
The data exporter is:
[This section is deemed to be populated with your details]

Data importer
The data importer is:
[This section is deemed to be populated with our details or the relevant Telstra Group Company]

Data subjects
The personal data transferred concern the following categories of data subjects:
[This section is deemed to be populated with the content of the section headed "The categories of Data Subject to whom your Personal Data relates" in ANNEX 1 to this Addendum]

Categories of data
The personal data transferred concern the following categories of data:
[This section is deemed to be populated with the content of the section headed "The types of your Personal Data to be Processed" in ANNEX 1 to this Addendum]

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
[This section is deemed to be populated with the content of the section headed "The types special categories of your Personal Data to be Processed " in ANNEX 1 to this Addendum]

Processing operations
The personal data transferred will be subject to the following basic processing activities:

The processing operations are set out in the Agreement.
DATA EXPORTER

[*Populated with details of, and deemed to be signed on behalf of, the data exporter:*]
Name:……
Authorised Signature ……
DATA IMPORTER

[*Populated with details of, and deemed to be signed on behalf of, the data importer:*]
Name:……
Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Telstra Security Standards

Information Security Program

Telstra's Security Governance Framework (the **"Framework"**) provides a structured approach to leading and managing security-related business processes and activities within Telstra. The Framework has been developed to be better practice in the context of current industry and government practices in protective security governance, control and assurance. Telstra's protective security approach provides a combination of procedural, physical, personnel, and information security measures designed to provide information, functions, resources, employees and customers with protection against security threats.

The Framework defines a number of baseline controls covering areas such as ICT, physical, personnel, operational and assurance. Underpinned by a top-down risk management framework, these controls are implemented at appropriate risk based levels to protect the confidentiality, integrity and availability of both Telstra core and customer specific data.

The Framework (including the adoption and enforcement of internal policies and procedures) is designed to (a) help secure against accidental or unlawful data loss, access or disclosure (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the Telstra Network and (c) minimise security risks, including through risk assessment and regular testing. Telstra will designate one or more employees to coordinate and be accountable for the Framework and the Framework will include the following measures:

1.1 Network Security. Telstra's Network Security controls protect customer data and Telstra's products, services and tools from downtime due to malicious and unintentional failures. Telstra's Network Security Standard provides the minimum standards to be met for Network Security to ensure our customers have reliable service and their data is kept in confidence. The Telstra Network is electronically accessible to employees, contractors and any other person as necessary to providing services for Telstra. Telstra will manage access controls and policies to manage what access is allowed to the Telstra Network from each network connection and user. Telstra will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security and Access Controls. Telstra's Physical Security controls protect people, processes and technology from events that could cause loss or damage to Telstra. Telstra's Physical Security Standard provides the minimum standards that are to be met to control physical access to Telstra's electronically-held information. Telstra provides controlled access to corporate offices and data centres. Building access points are maintained securely and access points to premises are monitored. Telstra also employs detection systems designed to detect unauthorised access to buildings, including monitoring points of vulnerability to detect individuals attempting to gain access. Physical

access to buildings by employees and contractors is logged and routinely audited. Telstra's Access Control Standard provides the minimum standards that are to be met for access control.

1.3 Limited Employee and contractor access. Telstra provides access to buildings to those employees and contractors and suppliers who have a legitimate business reason for the access privileges. When an employee no longer has a legitimate business reason for the access rights assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of Telstra or its affiliates. Telstra's employment contracts contain confidentiality clauses and employees and contractors are provided with privacy and security training. Contracts with Telstra's engaged service providers include data security clauses that support adherence and alignment with our security standards.

1.4 Business Continuity. Telstra's Business Continuity Management (BCM) policy and framework is designed to ensure that effective and comprehensive business continuity arrangements are in place to protect Telstra's critical processes and functions. The program protects the interests of the company's critical stakeholders and customers by providing continuity of core operations. Telstra's business resilience program includes Operational Resilience, Recovery Planning, Crisis Management, Supplier Governance and Emergency Management.

1.5 Testing. Telstra reviews security controls and performs security testing that consists of both initial project acceptance and operational readiness testing as well as an ongoing testing program. Testing activities include but are not limited to: design validation, operational readiness, vulnerability assessments, vulnerability scanning, penetration testing and patch management.

2. Industry Standards

Telstra's Security Standards supporting the Framework align to a number of controls within industry practices and standards such as ISO/IEC 27001:2013, ISO 31000:2009, NIST and PCI DSS.

Telstra's corporate policies, processes and standards apply equally across the organisation including formally certified products and internally governed environments.

Telstra can provide details of our current certifications upon request from customers.

3. Continued Evaluation. Telstra conducts continuous improvement and conducts periodic reviews of the adequacy of its information Security Governance Framework as measured against industry security standards and its policies and procedures.