Data Processing Addendum

Digistorm Group - Version 1.0 – 16 January 2020

1 Background

(a) This Data Processing Addendum ("**Addendum**") forms part of our Master Agreement https://www.digistorm.com.au/legal/master-agreement-2.0.pdf, as updated or amended from time to time ("**Agreement**"), between you, the Organisation and us.

(b) All capitalised terms not defined in this Addendum have the meaning set out in the Agreement.

(c) This Addendum only applies if and to the extent we process personal data on your behalf and you qualify as a controller with respect to that personal data under the GDPR.

(d) This Addendum has been pre-signed by us. To enter into this Addendum, you must:

(i) have entered into an Agreement with us;

(ii) complete the signature block in Part 3 of this Addendum by signing and completing all noted items; and

(iii) submit the completed and signed Addendum to us at legal@digistorm.com.

(e) This Addendum will only be effective once signed and returned as required, as confirmed by our email server, and will be effective from that date. If you make any deletions or other revisions to this Addendum, then this Addendum will be null and void.

(f) The person signing on your behalf represents to us that he or she has the legal authority to bind your corporate entity to this Addendum and is lawfully able to enter into contractual arrangements. We will rely on this representation.

(g) This Addendum will terminate automatically upon the termination of the Agreement or as earlier terminated pursuant to the terms of this Addendum.

2 Data Protection

2.1 Definitions

In this Addendum, the following terms have the following meanings:

(a) **controller**, **processor**, **data subject**, **personal data**, **processing** (and **process**) and **special categories of personal data** have the meanings given in the GDPR;

(b) **GDPR** means the EU General Data Protection Regulation (Regulation 2016/679) and any applicable national laws made under the GDPR;

(c) **Organisation** has the same meaning in the Agreement;

(d) **you** and **your** means the Organisation; and

(e) **us**/**our**/**we** means the Licensor contracting party from the Agreement.

2.2 Relationship of the parties

(a) You, the controller, appoint us as a processor to process the personal data described in Annexure B ("**Data**") only on your documented instructions (and as per the terms set out in this Addendum) for the purposes described in the Agreement or as otherwise agreed in writing by the parties ("**Permitted Purpose**").

(b) Each party must comply with the obligations that apply to it under the GDPR.

2.3 Controller instructions

(a) You warrant that the instructions given to us are lawful and comply with the legal and regulatory provisions relating to data protection, including the GDPR.

(b) If you act as a processor on behalf of another controller ("**First Controller**"), then you warrant that your instructions are in accordance with the instructions that have been provided by the First Controller.

(c) We are not required to act on your instructions where we reasonably consider that the instruction or direction given by you would infringe any legal and/or regulatory provision on data protection, including the GDPR.

2.4 Sensitive data

(a) Under the Agreement and for the Permitted Use, you will collect and we may be required to process special categories of personal data ("**Sensitive Data**"). The Sensitive Data that you will collect and which we will process for the Permitted Purpose includes that as outlined in Annexure C.

(b) You must and expressly warrant to us that you have, obtained explicit consent from each data subject to process the Sensitive Data.

(c) We undertake to pay particular attention to the Sensitive Data and to implement security measures as required by the GDPR to ensure the confidentiality of the Sensitive Data, subject to the intended use of our Products and the Permitted Purpose.

2.5 International transfers

(a) We are established and process personal data outside of the European Economic Area ("**EEA**").

(b) The parties to this Addendum will ensure that adequate protective measures are taken in accordance with the GDPR prior to any transfer or processing of Data outside of the EEA.

(c) The transfer of Data from the EEA will occur to a country outside of the EEA which does not offer adequate protection as deemed by the European Commission, namely, Australia. Accordingly, the European Commission's Standard Contractual Clauses at Annexure D of

this Addendum ("**SCC's**") are incorporated and will bind the parties. The parties comply with the SCC's.

2.6 Confidentiality of processing

We will ensure that any person we authorise to process the Data ("**Authorised Person**") will protect the Data in accordance with our confidentiality obligations under the Agreement, including this Addendum.

2.7 Security

We will implement technical and organisational measures, as set out in Annexure A, which may be amended and updated from time to time, to protect the Data:

(a) from accidental or unlawful destruction; and

(b) loss, alteration, unauthorised disclosure of, or access to the Data ("**Security Incident**").

2.8 Subcontracting

You expressly consent to us engaging third-party subprocessors to process the Data for the Permitted Purpose provided that:

(a) we maintain an up-to-date list of subprocessors, which is available on our website at the https://www.digistorm.com.au/legal/privacy-policy/subprocessor-list.pdf, which we will update with details of any change in subprocessors at least 30 days prior to the change;

(b) we impose data protection terms on any subprocessor we appoint that require the third party to protect the Data to the standard required by the GDPR; and

(c) we remain liable for any breach of this Addendum that is caused by an act, error or omission of our subprocessor. You may object to our appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such an event, we will either not appoint or replace the subprocessor or, if we determine in our sole discretion that this is not reasonably possible, you may suspend or terminate the Agreement without penalty (without prejudice to any fees you have incurred up to and including the date of suspension or termination).

2.9 Cooperation and data subjects' rights

We will provide you with reasonable and timely assistance (at your expense) to enable you to respond to:

(a) any request from a data subject to exercise any of their rights under the GDPR; and

(b) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. If any such request, correspondence, enquiry or complaint is made directly to us, we will promptly inform you, providing full details.

2.10 Data Protection Impact Assessment

If we believe or become aware that we are processing Data that is likely to result in a high risk to the data protection rights and freedoms of data subjects, we will inform you and provide

reasonable cooperation to you in connection with any data protection impact assessment that may be required under the GDPR.

2.11 Security incidents

(a) If we become aware of a confirmed Security Incident, we will inform you without undue delay and will provide reasonable information and cooperation to you so that you can fulfil any data breach reporting obligations you may have under (and in accordance with the timeframes required by) the GDPR.

(b) We will further take reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident and keep you informed of all material developments in connection with the Security Incident.

2.12 Deletion or return of Data

We will retain the Data for a period of 7 years after a subscription is terminated in case you later require access to that account. On expiry of this period or on your earlier request, we will delete or return the Data in a manner and form decided by us, acting reasonably. This requirement will not apply to the extent that we are required by applicable law to retain some or all of the Data, or to Data we have archived on back-up systems, which Data we shall securely isolate and protect from any further processing.

2.13 Audit

(a) Subject to the confidentiality obligations set out in the Agreement and at your cost, we will allow the you and the auditors appointed by you to inspect and audit the processing activities of the Data and comply with any reasonable requests or instructions issued during or following such inspection.

(b) We will immediately inform the you of any audit or other control activity carried out by the data protection supervisory authorities at our premises in connection with the processing of the Data this Addendum. Subject to confidentiality and our trade secrets, the we shall communicate the conclusions of any official investigation to you. We will ensure that appropriate corrective measures, where technically possible, are immediately implemented and shall provide you with proof of such compliance.

3 Customer Signing (controller)

Please sign and return the enclosed copy of this Addendum as instructed to acknowledge the supplementation of these terms to the Agreement.

Customer	Customer Name: Signature: Name: Title: Date: Contact details:

4 Digistorm Signing (processor)

Notwithstanding the signature below of any other entity, an entity is not a party to this Addendum unless they are a party to the Agreement for the provision of the Products to you.

Data Protection Point of Contact: Tim Oswald

Contact details: legal@digistorm.com

Digistorm Pty Ltd	Signature: Name: Tim Oswald Title: Managing Director Date:
Digistorm, LLC	Signature: Name: Tim Oswald Title: Managing Director Date:

Annexure A – Security Measures

1. Access control to premises and facilities

Measures must be taken to prevent unauthorised physical access to premises and facilities holding personal data. Measures shall include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries

2. Access control to systems

Measures must be taken to prevent unauthorised access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators

3. Access control to data

Measures must be taken to prevent authorised users from accessing data beyond their authorised access rights and prevent the unauthorised input, reading, copying, removal modification or disclosure of data. These measures shall include:

- Differentiated access rights
- Access rights defined according to duties
- Automated log of user access via IT systems
- Measures to prevent the use of automated data-processing systems by unauthorised persons using data communication equipment

4. Input control

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.

Measures should include:

- Each employee being bound by a duty of confidentiality or subject to an appropriate legal obligation of confidentiality

5. Job control

Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

6. Availability control

Measures should be put in place designed to ensure that data are protected against accidental destruction or loss.

These measures must include:

- Installed systems may, in the case of interruption, be restored
- Systems are functioning, and that faults are reported
- Stored personal data cannot be corrupted by means of a malfunctioning of the system
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems

7. Segregation control

Measures should be put in place to allow data collected for different purposes to be processed separately.

These measures should include:

- Restriction of access to data stored for different purposes according to staff duties

- Segregation of IT testing and production environments

Annexure B – Data Processing Schedule

4.1 Nature and Purpose of Processing Personal Data

The nature and purpose of processing personal data is to enable the functionality of the Digistorm Products as set out in the Agreement, related documentation and on the Digistorm website.

4.2 Types of Personal Data Processed and categories of Data Subjects

(a) Direct identifying information (eg name, picture, email, phone numbers)

(b) Indirect identifying information (eg gender, date of birth, place of birth, language, nationality, tuition records, payment information)

(c) Device identification data and traffic date (eg IP addresses, MAC addresses, web logs)

(d) Any personal data supplied by end users of the Products

Annexure C – Sensitive Data

(a) Direct identifying information (eg medical reports, medical conditions).

(b) Indirect identifying information (eg religion, learning requirements, medication, custody/court orders).

(c) Any personal data supplied by end users of the Products.

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)

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

The Licensor (as defined in the Data Processing Addendum) (hereinafter the "**data importer**")

and

the Organisation (as defined in the Data Processing Addendum) (hereinafter the "**data exporter**")

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 Annexure B.

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;

(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 Annexure B and Annexure C 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 Annexure A 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;

(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 Annexure A, 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 Annexure A 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 Annexure A 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; and

(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.

4. The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

5. Indemnification is contingent upon:

   (a) the data exporter promptly notifying the data importer of a claim; and
   (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

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.

Appendix 1 to the Standard Contractual Clauses

Data exporter

The Organisation (as defined in the Data Processing Addendum)

Data importer

The Licensor (as defined in the Data Processing Addendum)

Data subjects

The personal data concern end users of the Products, in addition to individuals whose personal data is supplied by end users of the Products.

Categories of data

The personal data transferred concern the categories of data outlined in Annexure B of the Data Processing Addendum.

Special categories of data

The special categories of data transferred concern the categories of data outlined in Annexure C of the Data Processing Addendum.

Purposes of processing

The personal data is processed for the purposes of providing the Products in accordance with this Agreement.

Appendix 2 to the Standard Contractual Clauses

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

The technical and organizational security measures implemented by the data importer are as described in Annexure A of the Data Processing Addendum.