Data Protection Agreement

1. **INTERPRETATION**

1. In this Attachment:

"Controller"	shall have the meaning set out in the GDPR;
"Client"	means the contracting party with Morae.
"Client Data"	Means information or data which is provided to Morae by or on behalf of the Client for the purposes of performing a service under the agreed terms.
"Data Protection Laws"	means and includes the Privacy Act 1988 (Cth), the GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communication Regulations 2003, any amendment, consolidation or re-enactment thereof, any legislation of equivalent purpose or effect enacted in the United Kingdom, or, where relevant, the European Union, and any orders, guidelines and instructions issued under any of the above by relevant national authorities, a judicial authority in England and Wales or, where relevant, a European Union judicial authority. ;
"Data Breach"	shall have the meaning as set out in the Privacy Act 1988
"Data Subject"	shall have the meaning set out in the GDPR;
"Disclosing Party"	shall mean the party to this Agreement who discloses or makes available Personal Data.
"GDPR"	means General Data Protection Regulation (EU) 2016/679 as in force from time to time and, as applicable to the EEA and the United Kingdom, including any variations and adoptions of the regulation therein as Replacement National Legislation;
"Information Security Policy"	means a policy created and maintained by Morae which covered information security compliance and management for the proper functioning of Morae's core Systems.
"OAIC"	Means Office of the Australian Information Commissioner.
"Personal Data"	has the meaning given to it by the GDPR, but shall only include personal data to the extent that such personal data, or any part of such personal data, is processed in relation to the services provided under this Agreement;
"Processor"	shall have the meaning set out in the GDPR;

“Receiving Party”	shall mean the party to this Agreement who receives or obtains Personal Data whether directly from the Disclosing Party or indirectly;
"Replacement National Legislation"	means legislation in the United Kingdom which is enacted to cover, in whole or part, the same subject matter as the GDPR.

2. Words and phrases with defined meanings in the GDPR have the same meanings when used in this Attachment, unless otherwise defined in this Attachment.

3. If the GDPR ceases to apply to the United Kingdom, references to the GDPR, to provisions within it and to words and phrases with defined meanings in it, shall be deemed references to Replacement National Legislation, the nearest equivalent provisions in it and the nearest equivalent words and phrases in it (as the case may be).

2. OBLIGATIONS UNDER GDPR

1. Each party shall comply with the Data Protection Laws applicable to it in connection with this Agreement and shall not cause the other party to breach any of its obligations under Data Protection Laws.

2. The parties have agreed that the Receiving Party will process Personal Data as the Processor on behalf of the Disclosing Party which shall act as a Controller of such Personal Data in connection with this Agreement. The Processor shall, or shall ensure that its sub-contractor shall:

a. process the Personal Data only on behalf of the Controller, only for the purposes of performing its obligations under this Agreement, and only in accordance with instructions contained in this Agreement or instructions received in writing from the Controller from time to time. The Processor shall notify the Controller if, in its opinion, any instruction given by the Controller breaches Data Protection Laws or other applicable law;

b. not otherwise modify, amend or alter the contents of the Personal Data or disclose or permit the disclosure of any of the Personal Data to any third party (including without limitation the Data Subject itself) unless specifically authorised in writing by the Controller;

c. document all processing in accordance with Article 30 GDPR;

d. only grant access to the Personal Data to persons who need to have access to it for the purposes of performing this Agreement;

e. ensure that all persons with access to the Personal Data are:

i. reliable, trustworthy and suitably trained on Data Protection Laws; and

ii. subject to an obligation of confidentiality or are under an appropriate statutory obligation of confidentiality.

f. taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with its obligations pursuant to Article 32 to 36 GDPR inclusive;

g. as a minimum, take all measures required pursuant to Article 32 GDPR in accordance with best practice and the security obligations set out in this Agreement (as amended from time to

time), whichever imposes a higher standard, and at the request of the Controller provide a written description of, and rationale for, the technical and organizational measures implemented, or to be implemented, to:

i. protect the Personal Data against unauthorized or unlawful processing and accidental loss, destruction, damage, alteration or disclosure; and

ii. detect and report personal data breaches within good time,

such measures shall be subject to the adequacy assessment of the Controller. Where the Controller does not deem such measures adequate, the Processor shall revise them until the Controller does so. Once approved by the Controller, the Processor shall be bound to implement and maintain such measures, and shall provide the Controller with reasonable assistance in documenting its adequacy assessment;

h. report to the Controller on a regular basis, and at least once every year, on the status of the Personal Data security. These reports shall at least include the status of the data processing systems, the security measures, registered downtime of technical security measures and the required and/or recommended improvements;

i. notify any loss, damage or destruction of Personal Data to the Controller as soon as reasonably practicable and in any event within 24 hours of becoming aware of such breach and provide all reasonable assistance to the Controller in relation to the notification of such breach to the Information Commissioner and any other applicable regulator and any data subject;

j. provide all reasonable assistance to the Controller in ensuring compliance with its legal obligations relating to data security and privacy impact assessments.

k. not engage another processor (a "Sub-Processor") to process the Personal Data on its behalf without specific written consent of the Controller, approving a named Sub-Processor, such consent always subject to:

i. the Processor binding any Sub-Processor by written agreement, imposing on the Sub-Processor obligations in relation to the Personal Data equivalent to those set out in this Agreement; and

ii. the Processor remaining liable to the Controller for the acts and omissions of any Sub-Processor, as if they were the acts and omissions of the Processor;

l. notify the Controller (within seven days) if it receives:

i. a request from a Data Subject to have access to that person's Personal Data; or

ii. a complaint or request relating to the Controller's obligations under Data Protection Laws; or

iii. any other communication relating directly or indirectly to the processing of any Personal Data in connection with this Agreement;

m. not take action in relation to such communication, unless compelled by law or a regulator, without the Controller's prior approval, and shall comply with any reasonable instructions the Controller gives in relation to such communication;

n. provide the Controller with full co-operation and assistance in relation to any complaint or request made in respect of any Personal Data including (without limitation) by:

i. providing the Controller with full details of the complaint or request;

ii. complying with a data access request within the relevant timescales set out in the Data Protection Legislation but strictly in accordance with the Controller's instructions;

iii. providing the Controller with any Personal Data it holds in relation to a Data Subject making a complaint or request within the timescales required by the Controller;

iv. providing the Controller with any information requested by the Controller; and

v. assisting the Controller to respond or comply with the Controller's complaint or request;

o. on termination of this Agreement and otherwise at the Controller's request, delete or return to the Controller the Personal Data, and procure that any party to whom the Processor has disclosed the Personal Data does the same;

p. where reasonably possible, store the Personal Data in a structured, commonly used and machine-readable format;

q. not transfer Personal Data outside of the European Economic Area without the prior written consent of the Controller. Where the Controller consents to the transfer of Personal Data outside the European Economic Area, the Processor shall comply with:

i. the obligations of a controller under Articles 44 to 50 GDPR inclusive by providing an adequate level of protection to any Personal Data transferred; and

ii. any reasonable instructions of the Controller in relation to such transfer;

r. have a data protection officer where required by the GDPR, and where a data protection officer is not required, have a named individual that is responsible and available to deal with data protection issues as and when they arise in conjunction with the Controller; and

s. allow the Controller, or its external advisers (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the Processor's data processing activities and those of its relevant agents, group companies and sub contractors, and comply with all reasonable requests or directions by the Controller, and to the extent necessary provide the Controller with access to its premises during normal business hours to enable the Controller to verify and procure that the Processor is in full compliance with its obligations under this Attachment.

OBLIGATIONS UNDER PRIVACY ACT 1988

3. DATA PROTECTION & SECURITY

3.1 The Parties shall, in performing their obligations under this Agreement, comply in all respects with all relevant Data Protection Laws.

3.2 Morae acknowledges that Client Data is the sole and valuable property of the Client (and its clients, where applicable) and that any unauthorised disclosure, use or loss of it could give rise to damage to the Client (and its clients, where applicable).

3.3 Morae shall:

3.3.1 keep the Client Data confidential as per the agreed terms;

3.3.2 process, use, store or otherwise handle the Client Data:

3.3.2.1 only for the purpose described in the statement of work; and

3.3.2.2 in accordance with this agreed terms;

3.3.3 maintain an Information Security Policy that is reviewed at regular intervals to respond to changing threats and risks and to cater to technology advances and provide evidence of this to the Client;

3.3.4 not subcontract any part of the Services to any third party unless otherwise approved in writing by a representative of the Client,

3.3.5 except as permitted by this Agreement, take all reasonable steps to ensure that Client Data is not disclosed or communicated to, or accessed by, any third party without the written authority of the Client or it Representative;

3.3.6 not use or exploit (for itself or any other person) any of the Client Data for any reason except as necessary to perform the Services during or after the termination of the MSA;

3.3.7 limit access to Client Data to Representatives of Morae who need access to the Client Data in order to perform the Services and take all reasonable steps to eliminate the risk of unauthorised access, use or disclosure of the Client Data by those representatives;

3.3.8 comply with all requirements and procedures relating to the use and protection of the Client Data as specified by the Client from time to time;

3.3.9 take all reasonable precautions to prevent the introduction of any virus or other unauthorised computer program or code into the Client's computer systems.

3.3.10 In the event any of Morae's security measures are found to be inadequate (as a result of an audit undertaken by the Client), Morae shall take steps to remedy such inadequacy and provide proof of remediation to the Client.

3.4 Morae must, to the extent it is in receipt of or has access to any Client Data, use appropriate technical and organisational measures to protect against unauthorised or unlawful processing, and against accidental loss or destruction, of any Client Data.

4. DATA BREACH NOTIFICATION

4.1 Notification of Data Breach

Morae shall:

(a) immediately report to the Client any likely or actual:

(b) unauthorised access to, or unauthorised disclosure of, Client Data; or

(c) any loss of Client Data in circumstances where unauthorised access to, or unauthorised disclosure,

in connection with its obligations under this Agreement (each a **Data Breach**) immediately after becoming aware of the Data Breach and, in any event, within 24 hours of becoming aware of the Data Breach; and

(d) comply with all instructions of the Client in relation to that Data Breach.

4.2**Response to Data Breach**

After notifying the Client in accordance with clause 4.1 and unless instructed in writing by the Client otherwise, Morae shall:

4.4.1 immediately investigate and remedy the Data Breach;

4.4.2 immediately provide written notification to the Client of:

4.4.2.1 the identity and contact details of any persons or entities likely to be involved in the Data Breach;

4.4.2.2 a description of the suspected, likely or actual Data Breach that Morae has reasonable grounds to suspect or believe has happened;

4.4.2.3 the kinds of Client Data affected by the Data Breach;

4.4.2.4 whether the breach amounts to an actual or suspected Data Breach and if so act in accordance with Clause 4.3 of this Agreement.

4.4.3 provide the Client with all information, documents and assistance required by the Client in respect of the Data Breach;

4.4.4 provide the Client with ongoing updates with respect to the Data Breach until such time as the Client determines that the Data Breach has been remedied;

4.4.5 cooperate with all reasonable directions of the Client in relation to the Data Breach; and

4.4.6 not notify the OAIC or affected individuals of the Data Breach, unless directed in writing by an representative of the Client in accordance with clause 4.1 or required by Data Protection Legislation,

Morae will comply with these obligations at its own cost where it is responsible for the Data Breach or on a contributory basis where it has caused or contributed to the breach in question.

4.3 Notification of an Eligible Data Breach

Immediately after Morae becomes aware that there are reasonable grounds to believe that there has been a Data Breach in connection with its obligations under this Agreement, at the Clients' option as notified to Morae, Morae will either:

4.3.1 provide all necessary information, documents and assistance reasonably required by Client to assist Client to prepare such statements and notify such individuals and the Information Commissioner in respect of the Eligible Data Breach in accordance with Division 3B of Part IIIC of the Privacy Act; or

4.3.2 work cooperatively in good faith with the Client to prepare a proposed statement in accordance with section 26WK(3) of Part IIIC of the Privacy Act, obtain the Clients' written approval to that statement and the method of notification for issuing such statement to affected individuals and OAIC (such approval not to be unreasonably withheld or delayed), and, if so instructed, issue the statement to affected individuals and OAIC on behalf of itself and the Client.

Morae shall comply with these obligations where it is responsible for the Data Breach.

5 LIABILITY

5.1 Morae shall indemnify and keep indemnified the Client against all liabilities, costs, expenses, damages and losses suffered or incurred by it arising out of or in connection with the Morae's breach of this Agreement, unless such indemnity is prohibited on grounds of public policy. Notwithstanding anything stated elsewhere in this Agreement the Morae's liability in damages for breach under this Agreement shall be uncapped.

6 INTELLECTUAL PROPERTY RIGHTS

6.1 All intellectual property rights in the Personal Data vest and shall remain vested absolutely in the Disclosing Party, that transferred the relevant Personal Data to the Receiving Party.

6.2 Electronic media and other means of transport containing the Personal Data received by the Receiving Party and all copies or reproductions thereof shall also remain the property of the Disclosing Party, that transferred these media or provided other means of transport.