AMAI DIGITAL DATA PROCESSING AGREEMENT
(PROCESSOR)

This Amai Digital Data Processing Agreement ("**Agreement**") forms part of the Contract for Services (the "**Principal Agreement**") between

Amai Digital Pte Ltd
1 Raffles Place
#44-01A
One Raffles Place
Singapore (048616)
(the "**Processor**")

and

_____
_____
_____
(the "**Controller**")

(collectively, the "**Parties**")

WHEREAS:

A. The Controller wishes to engage the Processor in providing the Services that include the Processing of the Personal Data by the Processor on behalf of the Controller; and
B. The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the GDPR; and
C. The Parties wish to lay down their rights and obligations with regard to the Processing of Personal Data within the scope of the Services.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1. "Agreement" means this Data Processing Agreement and all of its annexes;

1.1.2. "Service Data" means any Personal Data Processed by a the Processor on behalf of the Controller pursuant to or in connection with the Services;

1.1.3. "Data Protection Law" means applicable EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.4. "EEA" means the European Economic Area;

1.1.5. "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.6. "Services" means the following services the Processor provides, including, without limitation:

1.1.6.1. Development of apps and websites;

1.1.6.2. Maintenance and troubleshooting of apps and websites; and

1.1.6.3. Software consultancy services in relation to 1.1.6.1 and 1.1.6.2;

1.1.7. "Subprocessor" means an entity that Processes the Personal Data as a subcontractor of the Processor; and

1.1.8. "Instructions" means instructions issued by the Controller to the Processor and directing the Processor to perform a specific action with regard to the Processing of the Service Data in order to achieve compliance with the Data Protection Laws; and

1.1.9. The terms "Commission", "Data Subject", "Personal Data", "Personal Data Breach", and "Processing" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Subject matter of Processing

1.1. The Controller hereby engages the Processor to provide the Services to the Controller by means of the Principal Agreement and agrees that the Processor shall carry the Processing of the Service Data, the categories of which are described in Section 3 of this Agreement, pursuant to the terms stated herein.

1.2. The scope, extent, and nature of the Processing are the sole purpose of facilitation of the provision of the Services by the Processor to the Controller.

1.3. This Agreement stipulates the rights and obligations of the Parties with regard to the Processing of the Service Data in connection with the Services. It shall apply to all activities within the scope of the Services where the Processor or the Sub-Processors may come into contact with the Service Data.

1.4. To ensure the transparency of the Processing, the Parties shall keep records of all Processing activities regarding Personal Data as required by Art. 30 of the GDPR.

1.5. The Processor shall:

1.5.1. comply with the applicable Data Protection Law in the Processing of the Service Data;

1.5.2. not Process the Service Data other than on the relevant Controller's documented Instructions;

1.5.3. process the Service Data only to the extent required and with the purpose of fulfilling Processor's obligations under the Principal Agreement, to the extent necessary for the provision of the Services, and in accordance with the Instructions.

1.6. The Controller shall be responsible for complying with the applicable Data Protection Law, including, but not limited to, the lawfulness of the Processing and the lawfulness of the transmission (if any) of the Service Data to the Processor.

1.7. Should the Processor wish to use the Service Data for the purposes that are not specified in this section 2, the Processor shall request the Controller t to provide prior consent in writing.

1. Categories of Personal Data

1.1. The Processor shall Process all Service Data submitted by Controller within the scope of the Services. To the extent the Service Data contains Personal Data, it may consist of Data Subjects' identifying information, such as first names, last names, addresses, email addresses, and phone numbers, and other Personal Data submitted by the Controller.

1.2. No special categories of Personal Data as defined in Art. 9(1) of the GDPR shall be processed according to this Agreement.

2. Categories of Data Subjects

2.1. The affected Data Subjects shall include natural persons whose personal data is supplied by the Controller to the Processor within the scope of the Services.

2.2. The Processor does not and shall not interact with the Data Subjects directly in any manner.

3. Duration of Processing

3.1. Except where this Agreement expressly stipulates any surviving obligation, this Agreement shall follow the term of the Principal Agreement.

3.2. The Processor shall Process the Service Data for as long as the Service Data is necessary for the purpose described in Section 2 of this Agreement.

3.3. The Processor shall return to the Controller or securely erase the Service Data from its storage systems as soon as the Service Data is no longer necessary for the purpose described in section 2 of this Agreement or the Controller requests the Processor to do so. Upon request of the Controller, the Processor shall provide the Controller with a proof of erasure of the Service Data.

4. Correction and deletion of Personal Data

4.1. The Processor may be required by the Controller to correct, erase and/or block the Service Data if and to the extent the functionality of the Services do not allow the Controller to do so. However, the Processor shall not correct, erase or block the Service Data, unless instructed by the Controller.

4.2. Unless the Data Protection Law provides otherwise, there shall not be any direct communication between the Data Subjects and the Processor. In the event that a Data Subject does apply directly to the Processor in writing, e.g., to request the correction or deletion of his/her Personal Data, the Processor shall forward this request to the Controller without undue delay and shall not respond directly to the Data Subject.

5. Processor Personnel

5.1. The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Service Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Service Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with applicable laws in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. Security

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in relation to the Service Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

6.2. In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by the Processing, in particular from a Personal Data Breach.

6.3. The Processor shall appropriately document the technical and organisational measures actually implemented (including each update) for the Processing of the Service Data.

6.4. Any significant changes to Processor's security measures shall be documented by the Processor and reported to the Controller.

6.5. If the Processor is compelled to disclose the Service Data by a public authority as required by the Data Protection Law, the Processor shall inform the Controller before any such mandatory disclosure within 24 hours after such a disclosure is requested.

7. Subprocessing

7.1. The Controller hereby authorises the Processor to engage the Subprocessors specified in Processor's privacy policy, provided that the Processor remains responsible for any acts or omissions of its Subprocessors in the same manner as for its own acts and omissions hereunder. The Processor shall pass on to its subcontractors acting as the Subprocessors Processor's obligations under this Agreement.

7.2. The Processor shall not appoint (or disclose any Service Data to) any Subprocessor unless required or authorized by the Controller or the Service Data is strictly necessary for the purposes specified in section 2 of the Agreement.

7.3. The Processor may remove or appoint suitable and reliable other Subprocessor(s) at its own discretion in accordance with the following conditions:

7.3.1. The Processor shall inform the Controller 30 days in advance of any envisaged changes to the list of Subprocessors;

7.3.2. If the Controller has a legitimate data protection related reason to object to Processor's use of Subprocessor(s), the Controller shall notify the Processor within fourteen (14) days after receipt of the Processor's notice;

7.3.3. If the Controller does not object during this time period, the new Subprocessor(s) shall be deemed accepted;

7.3.4. If the Controller objects to the use of the Subprocessor(s) concerned, the Processor shall have the right to cure the objection through one of the following options (to be selected at Processor's sole discretion):

i. The Processor will abort its plans to use the Subprocessor(s) with regard to the Service Data; or

ii. The Processor will take corrective steps and proceed to use the Subprocessor(s) with regard to the Service Data.

7.3.5. If the Processor decides not to implement option 9.3.4.i or 9.3.4.ii above, the Processor shall notify the Controller without undue delay. In this case, the Controller shall be entitled within further fourteen (14) days to notify in writing the Processor about its termination of the Agreement and any such termination would become effective upon the expiry of the second (2^{nd}) calendar month after Processor's receipt of the termination notice.

8. Data Subject Rights

8.1. Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Controller's obligations, as reasonably understood by the Controller, to respond to requests to exercise Data Subjects' rights under the Data Protection Law.

8.2. The Processor shall:

8.2.1. promptly notify the Controller if it receives a request from a Data Subject under any Data Protection Law in respect of the Service Data; and

8.2.2. ensure that it does not respond to that request except on the documented instructions of the Controller or as required by the Applicable Law to which the Processor is subject, in which case Processor shall to the extent permitted by the applicable laws inform the Controller of that legal requirement before the Processor responds to the request.

9. Personal Data Breach

9.1. The Processor shall notify the Controller within twenty four (24) hours upon Processor's becoming aware of a Personal Data Breach affecting the Service Data, providing the Controller with sufficient information to allow the Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Law.

9.2. The Processor shall co-operate with the Controller and take reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

10. Data protection impact assessment and prior consultation

10.1. The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with competent data protection authorities, which the Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to the Processing of the Service Data by, and taking into account the nature of the Processing and information available to, the Processor.

11. Deletion or return of Service Data

11.1. The Processor shall promptly and in any event within ten (10) business days of the date of cessation of any Services involving the Processing of the Service Data, delete and procure the deletion of all copies of the Service Data.

12. Audit rights

12.1. The Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller in relation to the Processing of the Service Data by the Processor.

12.2. Information and audit rights of the Controller only arise to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

13. Data transfer

13.1. The Processor may not transfer or authorize other parties to the transfer of the Service Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Controller.

13.2. If the Service Data is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data that are attached to this Agreement as Annex I.

14. General terms

14.1. **Confidentiality.** Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

i. disclosure is required by law;

ii. the relevant information is already in the public domain.

14.2. **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

15. Governing Law and Jurisdiction

15.1. This Agreement is governed by the laws of Singapore.

15.2. Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Singapore, subject to possible appeal to Courts of Appeal of Singapore.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

THE PROCESSOR	**THE CONTROLLER**
Amai Digital Pte Ltd	_____
Signature _____	Signature _____
Name _____	Name _____
Title _____	Title _____
Date Signed _____	Date Signed _____

ANNEX I

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
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

Name of the data exporting Organization: *the name of the the entity using the services provided by Amai Digital Pte Ltd*

Address: *the address of the entity using the services provided by Amai Digital Pte Ltd*

Tel.: *the phone number of the entity using the services provided by Amai Digital Pte Ltds*

E-mail: *the email address of the using the entity using the services provided by Amai Digital Pte Ltd*

(the data **exporter**)

And

Name of the data importing Organization: *Amai Digital Pte Ltd*

Address: *1 Raffles Place, #44-01A, One Raffles Place, Singapore (048616)*

Tel.:

E-mail: *support@amai.com*

Other information needed to identify the Organization:

(the data **importer**)

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[1];

(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

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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 Organizational 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;

(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[2]

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 Organizational 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

---

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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[3]. 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

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 (please specify briefly your activities relevant to the transfer): *a business entity using the software applications, design, development, and consultation services provided by the data importer.*

Data importer

The data importer is (please specify briefly activities relevant to the transfer): *the provider of software*

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

applications and software design, development, and consultation services (https://amai.com).

Data subjects

The personal data transferred concern the following categories of data subjects (please specify): *the affected data subjects include natural persons whose personal data is submitted by the data exporter to the data importer within the scope of the services provided by the data importer to the data exporter.*

Categories of data

The personal data transferred concern the following categories of data (please specify): first names, last names, addresses, email addresses, and phone numbers *and other personal data submitted by the data exporter within the scope of the services provided by the data importer.*

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify): *no special categories of data as defined in Art. 9(1) of the GDPR should be submitted by the data exporter.*

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): *collection, recording, organisation, structuring, storage, retrieval, consultation, use, disclosure by transmission, dissemination and otherwise making available personal data within the scope of the services provided by the data importer to data exporter.*

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) (or document/legislation attached):

1. *Secured networks;*
2. *SSL encryption;*
3. *Strong passwords;*
4. *Limited access to personal data by data importer's staff; and*
5. *Anonymisation of personal data (when possible).*

INDEMNIFICATION CLAUSE

Liability

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.

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[4].

[4] Paragraph on liabilities is optional.