Data Protection Agreement

This Data Protection Addendum ("DPA") forms part of the Master Subscription Agreement ("Agreement") executed between Client and Supplier.

Capitalized terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

1. Definitions

1.1 In this DPA, the following terms shall have the meanings set out below:

1.1.1 "Applicable Laws" means any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data;

1.1.2 "CCPA" means the California Consumer Privacy Act of 2018;

1.1.3 "Client Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Client pursuant to or in connection with the Agreement;

1.1.4 "Contracted Processor" means Supplier or its Subprocessors;

1.1.5 "EEA" means the European Economic Area;

1.1.6 "EEA Data Protection Laws" means the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

1.1.8 "Personal Data" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a natural person;

1.1.9 "Restricted Transfer" means a transfer of Client Personal Data to Supplier; or an onward transfer of Client Personal Data from Supplier to a Subprocessor where such transfer would be prohibited by EEA Data Protection Laws in the absence of sufficient safeguards or a derogation from the applicable prohibition;

1.1.10 "Standard Contractual Clauses" means the contractual clauses set out in Annex 2;

1.1.11 "Subprocessor" means any person (including any third party, but excluding any affiliate or employee of Supplier) appointed by or on behalf of Supplier to Process Client Personal Data on behalf of Client in connection with the Agreement; and

1.2 The terms "Data Subject," "Processing," and "Supervisory Authority" shall have the same meaning as in the GDPR.

2. Processing of Client Personal Data

2.1 Supplier shall:

2.1.1 comply with all Applicable Laws in the Processing of Client Personal Data; and

2.1.2 not Process Client Personal Data other than pursuant to Client's documented instructions, including with regards to transfers of personal data to a third country or an international organization, unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Supplier shall, to the extent permitted by Applicable Laws, inform Client of that legal requirement before Processing that Client Personal Data.

2.1.3 where processing Client Personal Data within scope of the CCPA, Supplier will process Client Personal Data on behalf of Client and, not retain, use, disclose, or sell that Client Personal Data for any purpose, including for any commercial purpose, other than for the purposes set out in this DPA or as otherwise permitted by the CCPA or by the regulations promulgated by the California Attorney General pursuant to Cal. Civ. Code § 1798.185.

2.1.4 not be responsible for ensuring Client has a legal basis for processing Client Personal Data. It shall be Client's responsibility to ensure that it has an appropriate legal basis on which to Process Client Personal Data.

2.2 Client shall:

2.2.1 Provide notices to Data Subjects in accordance with Applicable Laws and, if required, obtain explicit consent from Data Subjects, by way of a clear affirmative action, or ensure other valid legal bases for processing in accordance with section 2.2.2.

2.2.2 Ensure that it has an appropriate legal basis on which to Process Client Personal Data.

2.3 Annex 1 to this DPA sets out certain information regarding the Contracted Processors' Processing of Client Personal Data as required by article 28(3) of the GDPR. Client may make reasonable amendments to Annex 1 by written notice to Supplier from time to time as Client reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this DPA.

3. Supplier Personnel

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

4. Security

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

5. Subprocessing

5.1 Client authorizes Supplier to appoint Subprocessors in accordance with this section 5 and any terms in the Agreement.

5.2 Supplier may continue to use those Subprocessors already engaged by Supplier as at the date of this DPA, subject to Supplier meeting the obligations set out in section 5.4.

5.3 Supplier shall give Client prior notice of the appointment of any new Subprocessor including full details of the Processing to be undertaken by the Subprocessor and provide Client with a reasonable opportunity to object to any changes to Supplier's Subprocessors.

5.4 With respect to each Subprocessor, Supplier shall:

5.4.1 before the Subprocessor first Processes Client Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Client Personal Data required by the Agreement;

5.4.2 ensure that the arrangement between Supplier and the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Client Personal Data as those set out in this DPA and meet the requirements of article 28(3) of the GDPR; and

5.4.3 if that arrangement involves a Restricted Transfer without sufficient safeguards, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between Supplier and Subprocessor.

5.5 Supplier shall ensure that each Subprocessor performs the obligations under sections 2.1, 4, 5, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Client Personal Data carried out by that Subprocessor, as if that Subprocessor were party to this DPA in place of Supplier.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Supplier shall assist Client by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligations, as reasonably understood by Client, to respond to requests to exercise Data Subject rights under EEA Data Protection Laws.

6.2 Supplier shall:

6.2.1 notify Client within a reasonable time if any Contracted Processor receives a request from a Data Subject under any EEA Data Protection Law with respect to Client Personal Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Client or as required by Applicable Laws to which the Contracted Processor is subject, in which case Supplier shall, to the extent permitted by Applicable Laws, inform Client of that legal requirement before the Contracted Processor responds to the request.

7. Security Incident Notification

7.1 Supplier shall notify Client without undue delay upon Supplier becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data, providing Client with sufficient information to allow it to meet any obligations to report or inform Data Subjects or Supervisory Authorities of the Personal Data Breach under EEA Data Protection Laws. For the avoidance of doubt, Supplier shall not notify Client of actions or activities that do not compromise the security of Client Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

7.2 Supplier shall reasonably cooperate with Client to assist in the investigation, mitigation, and remediation of any such breach of security described in section 7.1

8. Data Protection Impact Assessment and Prior Consultation

Supplier shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Client reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other EEA Data Protection Laws, in each case solely in relation to Processing of Client Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Client Personal Data

9.1 Supplier shall within a reasonable time after the date of cessation of any Services involving the Processing of Client Personal Data (the "Cessation Date"), at Client's option either:

9.1.1 Delete all copies of those Client Personal Data, or

9.1.2 Return all Client Personal Data to Client.

9.2 Supplier may retain a copy of Client Personal Data where required by Applicable Laws, and only to the extent and for such period as required by Applicable Laws and always provided that Supplier shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage.

10. Audit rights

10.1 Subject to section 10.2, Supplier shall make available to Client on request the information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Client or an auditor mandated by Client in relation to the Processing of Client Personal Data by the Contracted Processors.

10.2 Client may request, no more than once annually:

10.2.1 any written technical documentation that Supplier makes available or generally provides to its customer base; and

10.2.2 information regarding Supplier’s compliance with the obligations in this DPA, in the form of relevant third-party certifications and audit reports.

10.3 If, after Client’s review of the written records described in section 10.2 above, Client reasonably believes, in good faith, that an on-site audit is necessary to validate Supplier’s compliance with this DPA, Client may contact Supplier to request an audit of the procedures relevant to the protection of Client Personal Data.

10.4 Client shall give Supplier reasonable notice of any audit or inspection to be conducted under section 10.3. Before the commencement of any audit, Client and Supplier shall mutually agree upon the scope, timing, and duration of the audit in addition to the reasonable reimbursement rate for which Client shall be responsible. Client shall make (and ensure that each of its mandated auditors makes) reasonable efforts to avoid causing any damage, injury or disruption to the Contracted Processors’ premises, equipment, personnel and business 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:

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

10.4.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Client has given notice to Supplier that this is the case before attendance outside those hours begins; or

10.4.3 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:

10.2.3.1 Client demonstrates as being necessary because of Supplier’s non-compliance with this DPA; or

10.4.3.2 Client is required to carry out by EEA Data Protection Laws or a Supervisory Authority.

10.5 Client shall promptly provide Supplier with information regarding any non-compliance discovered during the course of an audit.

11. Cross-Border Transfers

11.1 Client authorizes Supplier to transfer Client Personal Data to any country or territory as reasonably necessary for the provision of the Services and consistent with the Agreement.

11.2 Supplier shall not transfer Client Personal Data to, Process Client Personal Data in, nor access Client Personal Data from, any country outside of the EEA except in accordance with EEA Data Protection Laws (which may include entering into the Standard Contractual Clauses for any Restricted Transfer).

11.3 If relied upon, the Standard Contractual Clauses shall come into effect under section 11.1 on the later of:

11.3.1 the data exporter becoming a party to them;

11.3.2 the data importer becoming a party to them; and

11.3.3 commencement of the relevant Restricted Transfer.

12. General Terms

Order of precedence

12.1 Nothing in this DPA modifies Supplier’s obligations under the Agreement in relation to the protection of Client Personal Data or permits Supplier to Process (or permit the Processing of) Client Personal Data in a manner prohibited by the Agreement.

12.2 Subject to section 12.1, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

Severance

12.3 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision(s) shall be either (i) amended as necessary to ensure its/their 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(s) had never been contained therein.

ANNEX 1: DETAILS OF PROCESSING OF CLIENT PERSONAL DATA

This Annex 1 includes certain details of the Processing of Client Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Client Personal Data

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

The nature and purpose of the Processing of Client Personal Data

Supplier processes Client Personal Data to provide products and services to Client.

The types of Client Personal Data to be Processed

Any Personal Data provided by Client to Supplier in connection with the Agreement.

The categories of Data Subject to whom the Client Personal Data relates

Users.

The obligations and rights of Client

The obligations and rights of Client are set out in the Agreement and this DPA.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

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 organisation: __________________

Address:

Tel.: ____________; fax: __________________; e-mail: __________________

Other information needed to identify the organisation

……………………………………………………………
(the data **exporter**)

And

Name of the data importing organisation: Digital.ai

Address:

Tel.: __________; fax: _____________; e-mail: _____________________

Other information needed to identify the organisation:

…………………………………………………………………
(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.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

1. '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;

2. 'the data exporter*'* means the controller who transfers the personal data;

3. '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;

4. '<u>the subprocessor</u>' 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;

5. '<u>the applicable data protection law</u>' 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 jurisdiction in which the data exporter is established;

6. '<u>technical and organisational security measures</u>' 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:

1. 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 jurisdiction where the data exporter is established) and does not violate the relevant provisions of that State;

2. 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;

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

4. 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;

5. that it will ensure compliance with the security measures;

6. 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;

7. 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;

8. 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;

9. 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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

1. 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;

2. 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;

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

4. that it will promptly notify the data exporter about:

a. 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,

b. any accidental or unauthorised access, and

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

5. 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;

6. 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;

7. 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;

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

9. that the processing services by the subprocessor will be carried out in accordance with Clause 11;

10. 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 jurisdiction 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 jurisdiction 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 jurisdiction 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:

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:

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.

Data exporter

The data exporter is: Client

Data importer

The data importer is: Supplier

Data subjects

The personal data transferred concern the following categories of data subjects:

Users.

Categories of data

The personal data transferred concern the following categories of data:

Identifiers, authentication data/credentials, contact information.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

None.

Processing operations

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

Provision of Supplier's products and services pursuant to the Agreement.

DATA EXPORTER

Name: ____________________ Authorised Signature: ____________________

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 4.3 and 4.8 and 5.3 of Annex 2:

The data importer has implemented and will maintain appropriate commercially reasonable technical and organizational measures, internal controls, and information security processes intended to protect Client Personal Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

DATA EXPORTER

Name: ____________________ Authorised Signature: ____________________

DATA IMPORTER

Name: ____________________ Authorised Signature: ____________________