HEXASOFT
DATA PROCESSING ADDENDUM
Controller-to-Controller

Published: May 20, 2018
Last Revised: June 15, 2022

This Hexasoft Data Processing Addendum (this "**Addendum**"), including its exhibits, is entered into by and between Hexasoft Development Sdn. Bhd. ("**Hexasoft**") and you ("**you**" or "**Client**") (each, a "**Party**" and, collectively, the "**Parties**"). If you are accepting the terms of this Addendum on behalf of an entity, you represent and warrant that you have the authority to bind such entity and its Affiliates, where applicable, to the terms of this Addendum. You are deemed to have accepted this Addendum on the later of the date on which you have accepted the Hexasoft End User License Agreement ("**EULA**"), or the published date as indicated above (the "**Effective Date**").

RECITALS

WHEREAS the Parties entered into the EULA which involves the Processing of certain Personal Data of Data Subjects which the Parties wish to amend as provided in this Addendum;

WHEREAS, in the course of performance of the EULA, Hexasoft transfers, transmits, and otherwise Processes Personal Data of Data Subjects;

WHEREAS, in connection with receiving Services under the EULA, the Client transfers, transmits, and otherwise Processes Personal Data of Data Subjects;

WHEREAS, each Party requires the other Party to take all necessary measures to handle Personal Data in compliance with Applicable Data Protection Law and enter into this Addendum with the intent to ensure such compliance.

NOW, THEREFORE, in consideration of the mutual agreements set forth in this Addendum, the Parties agree as follows:

1. Definitions

1.1. Capitalized definitions not otherwise defined herein shall have the meaning given to them in the EULA. Except as modified or supplemented below, the definitions of the EULA shall remain in full force and effect.

1.2. For the purpose of interpreting this Addendum, the following terms (and their applicable cognates) shall have the meanings set out below:

(a) "**Affiliate**" means any entity within a controlled group of companies that directly or indirectly, through one or more intermediaries, is controlling, controlled by, or under common control with one of the Parties.

(b) "**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the EULA, including but not limited to the GDPR and the laws and regulations defined as Applicable Data Protection Laws in **Exhibit B** hereto.

(c) "**Contracted Processor**" means any third party appointed by or on behalf of a Controller to Process Personal Data on behalf of such Controller.

(d) "**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(e) "**GDPR**" or "**General Data Protection Regulation**" 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," as may be amended from time to time.

(f) "**Personal Data**" means any information relating to an identified or identifiable natural person (a "**Data Subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

(g) "**Personal Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

(h) "**Personal Data Recipient**" means, as applicable, a Party that imports Personal Data, one or more Contracted Processors engaged by or on behalf of a Party that imports Personal Data, or where applicable, both the Party that imports Personal Data and its Contracted Processor(s), collectively.

(i) "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

(j) "**Processor**" means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of a Controller.

(k) "**Restricted International Transfer**" means any transfer of Personal Data subject to Applicable Data Protection Laws to a Third Country (as defined under **Exhibit B** for each type of Restricted International Transfer) or an international organization in a Third Country (including data storage on foreign servers).

(l) "**Services**" means the services and other activities carried out by or on behalf of Hexasoft for Client pursuant to the EULA.

(m) "**Standard Contractual Clauses**" are the model clauses for Restricted International Transfers adopted by the relevant authorities of the jurisdictions indicated in **Exhibit B**, as further defined and specified therein.

2. Scope and Applicability

2.1. The terms of this Addendum shall take effect on the Effective Date and shall continue concurrently for the term of the EULA.

2.2. This Addendum serves as a framework for Personal Data Processing in connection with the EULA, as well as for the transfer of Personal Data between the Parties; it also defines the principles and procedures that the Parties shall adhere to and the respective responsibilities of the Parties.

2.3. This Addendum will not apply to the Processing of Personal Data where such Processing is not regulated by the Applicable Data Protection Laws.

3. Controllership Role

3.1. The Parties acknowledge and agree that in the context of this Addendum, each Party acts as an independent Controller with regards to the Processing of Personal Data under the EULA.

3.2. Each Party shall identify and comply with its respective obligations under this Addendum when Processing Personal Data.

4. Obligations of the Parties

4.1. When Processing Personal Data, each Party shall:

(a) only conduct Restricted Transfers in compliance with all relevant conditions under Applicable Data Protection Laws and as further outlined in **Exhibit B**;

(b) take reasonable steps to ensure the reliability of any employee, agent, or contractor of any Personal Data Recipient who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of the Processing, and to comply with Applicable Data Protection Laws in the context of that individual's duties to the Personal Data Recipient, ensuring that all such individuals are subject to formal confidentiality undertakings or professional or statutory obligations of confidentiality; and

(c) 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 to the rights and freedoms of natural persons, with regard to Personal Data, implement and maintain appropriate technical and organizational security 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, or the equivalent provisions of other Applicable Data Protection Laws. In assessing the appropriate level of security, each Party shall take into account, in particular, the sensitivity of the Personal Data and the risks that are presented by the nature of such Processing activities, particularly those related to possible Personal Data Breaches.

5. Controller Representations and Warranties

5.1. When Processing Personal Data as a Controller, each Party represents, warrants, and covenants that:

(a) all Personal Data has been and will be collected and otherwise Processed in compliance with Applicable Data Protection Laws;

(b) it will independently determine its obligations under Applicable Data Protection Laws;

(c) it will ensure that the Processing of the Personal Data is performed only on lawful grounds pursuant to Article 6 of the GDPR, and as further limited by Article 9 of the GDPR, or the relevant provisions of any Applicable Data Protection Laws, as the case may be;

(d) it will only engage a Contracted Processor to Process Personal Data on its behalf or share Personal Data with a third-party Data Controller if that Contracted Processor or third-party Data Controller provides sufficient guarantees to that Party, by way of a written contract, that it will duly account for all requirements of the GDPR and/or the relevant provisions of any Applicable Data Protection Laws, as the case may be;

(e) it will be responsible for responding to requests it receives related to the exercise of rights of the Data Subjects under Chapter III of the GDPR or the equivalent provisions of other Applicable Data Protection Laws, with regard to the Personal Data Processed by that Party, and also agrees to provide, upon the request of the other Party, prompt and reasonable assistance, where legally required or reasonably expected, to enable both Parties to comply with such Data Subject requests;

(f) it will promptly provide, where legally required or reasonably expected, all needed assistance to the other Party with respect to Personal Data Breaches;

(g) it will maintain a record of Processing activities of Personal Data under its responsibility, in accordance with Article 30, par. 1 of the GDPR; and

(h) it will, upon request of the other Party, provide copies of all relevant data protection laws or references to them (not including legal advice) that apply to it.

6. Jurisdiction Specific Terms

6.1. To the extent the Parties Processes Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions listed in **Exhibit B**, then the terms and definitions specified in **Exhibit B** with respect to the applicable jurisdiction(s) ("**Jurisdiction Specific Terms**") shall apply in addition to the terms of this Addendum.

6.2. Hexasoft may update **Exhibit B** from time to time to reflect changes in or additions to Applicable Data Protection Laws to which the Parties are subject. If Hexasoft updates **Exhibit B**, it will provide the updated **Exhibit B** to Client. If Client does not object to the updated **Exhibit B** within fourteen (14) days of receipt, Client will be deemed to have consented to the updated **Exhibit B**.

6.3. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this Addendum, the applicable Jurisdiction Specific Terms will prevail.

7. International Data Transfers

7.1. International transfers of Personal Data within the scope of this Addendum shall be conducted in accordance with the applicable terms and requirements of **Exhibit B**.

7.2. Where the Standard Contractual Clauses are the applicable data transfer mechanism according to the terms and requirements set out in **Exhibit B**, the applicable module of the Standard Contractual Clauses (if any) will be the module applicable to the role of the Parties as described in **Exhibit B**.

7.3. Hexasoft may update **Exhibits A and B** from time to time to reflect changes in or additions necessary to conclude the Standard Contractual Clauses. Without limiting the generality of the foregoing, if the execution of a new version of the Standard Contractual Clauses adopted by the relevant authorities in the jurisdiction governing the processing of Personal Data is later required in order for the Parties to rely on the Standard Contractual Clauses as a lawful mechanism for Restricted International Transfers, the Parties are deemed to have agreed to the new version of the Standard Contractual Clauses by signing this Addendum, and, if necessary, Hexasoft shall be entitled to update **Exhibits A and B** accordingly.

7.4. Hexasoft may update **Exhibit C** from time to time to provide for additional safeguards to Personal Data subject to the requirements of Applicable Data Protections Laws for Restriction International Transfers. If Hexasoft updates **Exhibit C**, it will provide the updated **Exhibit C** to Client. If Client does not object to the updated **Exhibit C** within fourteen (14) days of receipt, Client will be deemed to have consented to the updated **Exhibit C**.

8. Indemnification

8.1. Each Party (the "**Indemnifying Party**") agrees to indemnify and hold harmless the other Party and its officers, directors, employees, agents, affiliates, successors, and permitted assigns (the "**Indemnified Party**") against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind which the Indemnified Party may sustain as a consequence of the breach by the Indemnifying Party of its obligations pursuant to this Addendum and the Applicable Data Protection Laws.

9. General Terms

9.1. This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Hexasoft and Client in connection with the EULA.

9.2. All clauses of the EULA that are not explicitly amended or supplemented by the clauses of this Addendum remain in full force and effect and shall apply, as long as this does not contradict with compulsory requirements of Applicable Data Protection Laws under this Addendum.

9.3. In the event of any conflict between the EULA (including any annexes, exhibits, and appendices thereto) and this Addendum, the provisions of this Addendum shall prevail, except where the applicable Jurisdiction Specific Terms found in **Exhibit B** apply. In such

cases, the provisions of the applicable Jurisdiction Specific Terms found in Exhibit B shall take prevail over the terms of the EULA and the body of the Addendum.

9.4. Should any provision of this Addendum be found legally invalid or unenforceable, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the Addendum will continue in effect.

10. Hexasoft Data Protection Officer and Article 27 Representative

10.1. The Data Protection Officer of Hexasoft is:

Hexasoft Development Sdn. Bhd.
Attn: Data Protection Officer
70-3-30A D'Piazza Mall
Jalan Mahsuri
11950 Bayan Baru
Pulau Pinang
Malaysia

Email: support@fraudlabspro.com

10.2. The European Union Representative of Hexasoft pursuant to Article 27 of the EU GDPR is:

VeraSafe Czech Republic s.r.o.
Klimentská 46
Prague 1, 11002
Czech Republic

Contact form: https://verasafe.com/public-resources/contact-data-protection-representative

10.3. The United Kingdom ("**UK**") Representative of Hexasoft pursuant to Article 27 of the UK GDPR (as defined in the Jurisdiction Specific Terms) is:

VeraSafe United Kingdom Ltd.
37 Albert Embankment
London SE1 7TL

Contact form: https://verasafe.com/public-resources/contact-data-protection-representative

11. Client Data Protection Officer and Article 27 Representative

11.1. The Client shall, without undue delay after the Effective Data, provide Hexasoft, by way of sending an email to support@fraudlabspro.com, the following contact information for the Client's Data Protection Officer, GDPR Article 27 Representative, and/or UK GDPR Article 27 Representative, as applicable:

- Name and Surname;
- Designation;

- Email Address;
- Physical Address; and
- Telephone Number.

11.2. The Client shall promptly update, when necessary, the information provided in Section 11.1 above, and keep such information complete and up to date.

12. Notices Pursuant to this Addendum.

12.1. Notices to Hexasoft shall be sent to support@fraudlabspro.com, unless the Addendum indicated otherwise.

12.2. Notices to the Client shall be sent to the Client's email address associated with the Client's account and provided upon registration for the account associated with the Services.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

Exhibit A

Details of Processing

Further details of the Processing, in addition to those laid down in this Addendum, include:

1. **The categories of Data Subjects to whom the Personal Data relates are**:

   1.1. IP address, account identifier, order transaction information, browsing information, billing information and shipping information.

2. **The categories of Personal Data to be Processed are**:

   2.1. IP address, account identifier, order transaction information, browsing information, billing information and shipping information

3. **The Frequency of the transfer**:

   The frequency of the transfer is determined by the relevant data exporter in terms of **Exhibit B** and is further determined by the Services in accordance with the EULA.

4. **The nature and purpose of the Processing of Personal Data**:

   The purpose of the Processing of Personal Data is to facilitate the Services and flow of Personal Data between the Parties. The nature and purposes of Processing are further elaborated in the EULA.

5. **Further Processing of Personal Data**:

   Personal Data will generally be processed for the provision of the Services in terms of the EULA. Each Party, as an independent Controller, may further Process Personal Data, only in compliance with Applicable Data Protection Law and the terms of this Addendum.

6. **The period for which the Personal Data will be retained, or of that is not possible, the criteria used to determine that period**:

   The retention period for Personal Data is generally determined by each Party as independent Controllers and is further subject to the terms of this Addendum and the EULA.

7. **For transfer to Contracted Processors, also describe the specific technical and organizational measures to be taken by the Contracted Processors to be able to provide assistance to the Controller**:

   When a Party engages a Contracted Processor in terms of Section 5.1(d) of this Addendum, it is obligated to ensure that the Contractor Processor provides sufficient guarantees to that Party, by way of a written contract, that it will duly account for all requirements of the GDPR and/or the relevant provisions of any Applicable Data Protection Laws, as the case may be.

8. **The identity and contact information of Hexasoft's and Client's respective Data Protection Officer, EU Data Protection Representative, and UK Data Protection Representative (as applicable)**:

8.1. The identity and contact information of Hexasoft's Data Protection Officer, EU Data Protection Representative, and UK Data Protection Representative is set out in Section 10 of the Addendum.

8.2. The identity and contact information of the Client's Data Protection Officer, EU Data Protection Representative, and UK Data Protection Representative (as applicable) is set out in Section 11 of the Addendum.

Exhibit B

Jurisdiction Specific Terms

1. European Economic Area

1.1. Definitions

(a) "**Applicable Data Protection Laws**" (as used in the Addendum) includes EEA Data Protection Laws (as defined below).

(b) "**EEA**" (as used in this Section) means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.

(c) "**EEA Data Protection Laws**" means the EU GDPR and all laws and regulations of the EEA (as defined below), applicable to the Processing of Personal Data.

(d) "**EU 2021 Standard Contractual Clauses**" (as used in this Section) means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(e) "**Restricted International Transfer of EEA Personal Data**" (as used in this Section) means any transfer of Personal Data subject to the EU GDPR which is undergoing Processing or is intended for Processing after transfer to a Third Country (as defined below) or an international organization in a Third Country (including data storage on foreign servers).

(f) "**Standard Contractual Clauses**" (as used in the Addendum) includes the EU 2021 Standard Contractual Clauses.

(g) "**Third Country**" (as used in this Section) means a country outside of the EEA.

1.2. With regard to any Restricted International Transfer of EEA Personal Data between the Parties within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) A valid adequacy decision adopted by the European Commission on the basis of Article 45 of the EU GDPR that provides that the Third Country, a territory, or one or more specified sectors within that Third Country, or the international organization in question to which EEA Personal Data is to be transferred ensures an adequate level of data protection.

(b) The EU 2021 Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under Article 46 of the EU GDPR).

(c) Any other lawful data transfer mechanism, as laid down in the EEA Data Protection Laws, as the case may be.

1.3. EU 2021 Standard Contractual Clauses:

(a) This Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses. The Parties are deemed to have accepted, executed, and signed the Standard Contractual Clauses where necessary in their entirety (including the annexures thereto).

(b) The contents of the EU 2021 Annex I and Annex II of the EU 2021 Standard Contractual Clauses are set forth in **Exhibit A** to this Addendum.

(c) The text contained in **Exhibit C** of this Addendum supplements the EU 2021 Standard Contractual Clauses.

(d) The Parties agree to apply Module One (*Transfer controller to controller*) of the EU 2021 Standard Contractual Clauses when, in accordance with Section 3 of the Addendum, the Parties act as independent Controllers.

(e) For the purposes of Annex I.A:

i. One Party shall be deemed a "data exporter" and the other Party the "data importer" respectfully. For the purposes of clarity, a Party is a "data importer" where that Party is the receiving Party and a "data exporter" where it is the sending party, as applicable. In consideration of the fact that both Parties may send or receive Personal Data to and from each other, each Party is deemed to have entered into the EU 2021 Standard Contractual Clauses twice, as outlined in this Section 1.3(e)i), once as a "data importer" with the other Party being the "data exporter" and once with such roles reversed.

ii. The Parties have provided each other with the identity information contact details required under Annex I.A.

iii. The Parties' controllership roles are set forth in Section 3.1 of this Addendum.

iv. The details of the Parties' data protection officers and data protection representatives in the EU are set forth in **Exhibit A** and Sections 10 and 11 of this Addendum.

v. The activities relevant to the Personal Data transferred under the Standard Contractual Clauses are set forth in **Exhibit A** of this Addendum.

(f) The Parties' Choices under the EU 2021 Standard Contractual Clauses:

i. The Parties elect not to include Clause 7 of the EU 2021 Standard Contractual Clauses.

ii. With respect to Clause 11 of the EU 2021 Standard Contractual Clauses, the Parties agree not to provide the right to lodge a complaint with an independent dispute resolution body.

iii. With respect to Clause 17 of the EU 2021 Standard Contractual Clauses, the Parties select the law of the Republic of Ireland.

iv. With respect to Clause 18 of the EU 2021 Standard Contractual Clauses, the Parties agree that any dispute arising from the EU 2021 Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland.

1.4. For the purpose of Annex I.C and with respect to Clause 13 (when applicable) of the EU 2021 Standard Contractual Clauses:

(a) Hexasoft is not established in an EU Member State but falls within the territorial scope of Article 3(2) of the EU GDPR. Hexasoft has appointed a representative established in the Czech Republic pursuant to Article 27(1) of the EU GDPR, whose supervisory authority shall act as the competent supervisory authority and be responsible for ensuring compliance by Hexasoft with the GDPR as regards to the data transfer.

(b) In respect of the Client:

i. where the Client is established in an EU Member State, the competent supervisory authority shall be the authority for the EU Member State in which the Client is established;

ii. where the Client is not established in an EU Member State and has appointed a representative in an EU Member State pursuant to Article 27(1) of the EU GDPR, the competent supervisory authority shall be the authority for the EU Member State in which such representative is appointed; or

iii. where the Client is not established in an EU Member State and has not appointed a representative in an EU Member State pursuant to Article 27(1) of the EU GDPR, the competent supervisory authority shall be the authority in one of the EU Member States in which the Data Subject whose Personal Data in transferred under the EU 2021 Standard Contractual Clauses, in relation to the offering of goods or services to them, or whose behavior is monitored, are located.

1.5. In cases where the EU 2021 Standard Contractual Clauses apply and there is a conflict between the terms of the Addendum and the terms of the EU 2021 Standard Contractual Clauses, the terms of the EU 2021 Standard Contractual Clauses shall prevail.

2. United Kingdom

2.1. **Definitions**

(a) "**Applicable Data Protection Laws**" (as used in the Addendum) include UK Data Protection Laws (as defined below).

(b) "**Restricted International Transfer of UK Personal Data**" (as used in this Section) means any transfer of Personal Data subject to the UK GDPR to a Third Country (as defined below) or an international organization (including data storage on foreign servers).

(c) "**Standard Contractual Clauses**" (as used in the Addendum) include the EU 2021 Standard Contractual Clauses (as defined under Section 1 of this Exhibit).

(d) "**Third Country**" (as used in this Section) means a country outside of the United Kingdom.

(e) "**UK Addendum**" means the International Data Transfer Addendum to the EU 2021 Standard Contractual Clauses, issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022, as may be amended from time to time.

(f) "**UK Data Protection Laws**" (as used in this Section) include the Data Protection Act 2018 and the UK GDPR (as defined below).

(g) "**UK GDPR**" (as used in this Section) means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

2.2. With regard to any Restricted International Transfer of UK Personal Data between the Parties within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) A valid adequacy decision pursuant to Article 45 of the UK GDPR that provides that the Third Country, a territory, or one or more specified sectors within that Third Country or the international organization in question to which Personal Data is to be transferred ensures an adequate level of data protection.

(b) The EU 2021 Standard Contractual Clauses (as defined in Section 1 of this Exhibit), using the UK Addendum to the EU 2021 Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the UK Data Protection Laws).

(c) Any other lawful data transfer mechanism, as laid down in the UK Data Protection Laws, as the case may be.

2.3. EU 2021 Standard Contractual Clauses:

(a) This Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses and the UK Addendum. The Parties are deemed to have accepted, executed, and signed the Standard Contractual Clauses and the UK Addendum where necessary in their entirety (including the annexures thereto).

(b) The contents of EU 2021 Annex I and Annex II of the EU 2021 Standard Contractual Clauses and the tables of the UK Addendum are set forth in **Exhibit A** to this Addendum.

(c) The text contained in **Exhibit C** to this Addendum supplements the EU 2021 Standard Contractual Clauses.

(d) The Parties agree to apply Module One (*Transfer controller to controller*) of the the EU 2021 Standard Contractual Clauses when, in accordance with Section 3 of the Addendum, the Parties act as independent Controllers.

(e) For the purposes of Annex I.A:

i. One Party shall be deemed a "data exporter" and the other Party the "data importer" respectfully. For the purposes of clarity, a Party is a "data importer" where that Party is the receiving Party and a "data exporter" where it is the sending party, as applicable. In consideration of the fact that both Parties may send or receive Personal Data to and from each other, each Party is deemed to have entered into the EU 2021 Standard Contractual Clauses twice, as outlined in this Section 2.3(e)i), once as a "data importer" with the other Party being the "data exporter" and once with such roles reversed.

ii. The Parties have provided each other with the identity information and contact details required under Annex I.A.

iii. The Parties' controllership roles are set forth in Section 3.1 of this Addendum.

iv. The details of the Parties' data protection officers and data protection representatives (as applicable) in the UK are set forth in **Exhibit A** and Sections 10 and 11 of this Addendum.

v. The activities relevant to the Personal Data transferred under the Standard Contractual Clauses are set forth in **Exhibit A** to the Addendum.

(f) Parties' Choices under the EU 2021 Standard Contractual Clauses:

i. The Parties elect not to include Clause 7 of the EU 2021 Standard Contractual Clauses.

ii. With respect to Clause 11 of the EU 2021 Standard Contractual Clauses, the Parties agree not to provide the right to lodge a complaint with an independent dispute resolution body.

(g) In cases where the EU 2021 Standard Contractual Clauses apply and there is a conflict between the terms of the Addendum and the terms of the EU 2021 Standard Contractual Clauses, the terms of the EU 2021 Standard Contractual Clauses shall prevail.

2.4. The Parties agree that neither Party may end the UK Addendum as set out in Section 19 of the UK Addendum.

3. California

3.1. **Definitions**

(a) "**Applicable Data Protection Laws**" (as used in the Addendum) includes California Data Protection Laws, as may be amended from time to time.

(b) "**California Data Protection Laws**" includes the California Consumer Privacy Act of 2018, Assembly Bill 375 of the California House of Representatives, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy and approved by the California Governor on 28 June 2018 ("**CCPA**"), the California Privacy Rights Act ("**CPRA**") and the California Consumer Privacy Act Regulations ("**CCPA Regulations**"), as they may be amended from time to time.

(c) "**Personal Data**" (as used in the Addendum) includes "**Personal Information**" as defined under California Data Protection Laws.

(d) "**Controller**" (as used in the Addendum) includes "**Business**" as defined under the CPRA.

(e) "**Data Subject**" (as used in the Addendum) includes "**Consumer**" as defined under the CPRA.

(f) "**Personal Data Breach**" (as used in the Addendum) includes "**Breach of the Security of the System**" as defined under Section 1798.82(g) of the California Civil Code.

(g) "**Processor**" (as used in the Addendum) includes "**Service Provider**" as defined under the CCPA.

4. Brazil

4.1. **Definitions**

(a) "**Applicable Data Protection Laws**" (as used in the Addendum) includes "**Brazilian Data Protection Laws**" (as defined below).

(b) "**Brazilian Data Protection Laws**" (as used in this Section) includes the Lei Geral de Proteção de Dados, Law No. 13.709 of 14 August 2018 ("**LGPD**").

(c) "**Controller**" (as used in the Addendum) includes "**Controlador**" as defined under the LGPD.

(d) "**Personal Data Breach**" (as used in the Addendum) includes "**Security Incident**" as defined under the LGPD.

(e) "**Processor**" includes "**Operador**" as defined under the LGPD.

5. Canada

5.1. **Definitions**

(a) "**Applicable Data Protection Laws**" (as used in the Addendum) includes Canadian Data Protection Laws.

(b) "**Canadian Data Protection Laws**" includes the Canadian Federal Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), as they may be amended from time to time.

(c) "**Personal Data**" (as used in the Addendum) includes "**Personal Information**" as defined under PIPEDA.

(d) **"Contracted Processor**" (as used in the Addendum) includes "**Third Party Organization**" as defined under PIPEDA.

(e) "**Personal Data Breach**" (as used in the Addendum) includes "**Breach of Security Safeguards**" as defined under PIPEDA.

5.2. Each Party confirms that it has obtained a valid consent (as defined under PIPEDA) where necessary to Process Personal Data of each Data Subject.

6. Switzerland

6.1. **Definitions**

(a) "**Applicable Data Protection Laws**" (as used in the Addendum) includes Swiss Data Protection Laws, as they may be amended from time to time.

(b) "**Personal Data**" (as used in the Addendum) includes "**Personal Data**" as defined under the FADP.

(c) "**Controller**" (as used in the Addendum) includes "**Controller of the Data File**" as defined under the FADP.

(d) "**Processing**" (as used in the Addendum) includes "**Processing**" as defined under the FADP.

(e) "**Restricted International Transfer of Swiss Personal Data**" (as used in this Section) means any transfer of Personal Data (including data storage in foreign servers) subject to the FADP to a Third Country (as defined below) or an international organization.

(f) "**Standard Contractual Clauses**" (as used in the Addendum) includes the EU 2021 Standard Contractual Clauses (as defined under Section 1 of this Exhibit).

(g) "**Swiss Data Protection Laws**" includes the Federal Act on Data Protection of 19 June 1992 ("**FADP**") and the Ordinance to the Federal Act on Data Protection ("**OFADP**").

(h) "**Third Country**" (as used in this Section) means a country outside of the Swiss Confederation.

6.2. With regard to any Restricted International Transfer of Swiss Personal Data between the Parties within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) The inclusion of the Third Country, a territory, or one or more specified sectors within that Third Country, or the international organization in question to which Personal Data is to be transferred in the list published by the Swiss Federal Data Protection and Information Commissioner of states that provide an adequate level of protection for Personal Data within the meaning of the FADP.

(b) The EU 2021 Standard Contractual Clauses (as defined under Section 1 of this Exhibit) (insofar as their use constitutes an "appropriate safeguard" under Swiss Data Protection Laws).

(c) Any other lawful transfer mechanism, as laid down in Swiss Data Protection Laws.

6.3. EU 2021 Standard Contractual Clauses:

(a) This Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses. The Parties are deemed to have accepted, executed, and signed the Standard Contractual Clauses where necessary in their entirety (including the annexures thereto.

(b) The content of EU 2021 Annex I and Annex II of the EU 2021 Standard Contractual Clauses is set forth in **Exhibit A** to this Addendum.

(c) The text contained in **Exhibit C** to this Addendum supplements the EU 2021 Standard Contractual Clauses.

(d) The Parties agree to apply Module One (*Transfer controller to controller*) of the EU 2021 Standard Contractual Clauses when, in accordance with Section 3 of the Addendum, the Parties act as independent Controllers.

(e) For the purposes of Annex I.A:

i. One Party shall be deemed a "data exporter" and the other Party the "data importer" respectfully. For the purposes of clarity, a Party is a "data importer" where that Party is the receiving Party and a "data exporter" where it is the sending party, as applicable. In consideration of the fact that both Parties may send or receive Personal Data to and from each other, each Party is deemed to have entered into the EU 2021 Standard Contractual Clauses twice, as outlined in this Section 1.3(e)i), once as a "data importer" with the other Party being the "data exporter" and once with such roles reversed.

ii. The Parties have provided each other with the identity information contact details required under Annex I.A.

iii. The Parties' controllership roles are set forth in Section 3.1 of this Addendum.

iv. The details of the Parties' data protection officers (as applicable) are set forth in **Exhibit A** and Sections 10 and 11 of this Addendum.

v. The activities relevant to the Personal Data transferred under the EU 2021 Standard Contractual Clauses are set forth in **Exhibit A** to the Addendum.

(f) Parties' Choices under the EU 2021 Standard Contractual Clauses:

i. The Parties elect not to include Clause 7 of the EU 2021 Standard Contractual Clauses.

ii. With respect to Clause 11 of the EU 2021 Standard Contractual Clauses, the Parties agree not to provide the right to lodge a complaint with an independent dispute resolution body.

iii. For the purpose of Annex I.C and with respect to Clause 13 (when applicable) of the Standard Contractual Clauses, the competent authority shall be the Swiss Federal Data Protection and Information Commissioner, insofar as the data transfer constitutes as Restricted International Transfer of Swiss Personal Data.

iv. With respect to Clause 17 of the EU 2021 Standard Contractual Clauses, the Parties select the law of the Republic of Ireland.

v. With respect to Clause 18 of the EU 2021 Standard Contractual Clauses, the Parties agree that any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland. The Parties choose the Swiss courts as an alternative place of jurisdiction for Data Subjects habitually resident in Switzerland.

(g) The term "member state" included in the EU 2021 Standard Contractual Clauses must not be interpreted in such a way as to exclude Data Subject in Switzerland from the possibility of suing for the rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU 2021 Standard Contractual Clauses.

(h) The EU 2021 Standard Contractual Clauses also protect the data of legal entities until the entry into force of the revised FADP.

6.4. In cases where the EU 2021 Standard Contractual Clauses apply and there is a conflict between the terms of the Addendum and the terms of the EU 2021 Standard Contractual Clauses, the terms of the EU 2021 Standard Contractual Clauses shall prevail.

Exhibit C

Supplemental Clauses to the Standard Contractual Clauses

By this **Exhibit C** (this "**Exhibit**"), the Parties provide additional safeguards and redress to the Data Subjects whose Personal Data is transferred between the Parties pursuant to Standard Contractual Clauses. This Exhibit supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses that may be applicable to the Restricted International Transfer.

1. Applicability of this Exhibit

1.1. This Exhibit only applies with respect to Restricted International Transfers when the Standard Contractual Clauses apply to such Restricted International Transfers pursuant to the Addendum and its exhibits.

2. Definitions

2.1. For the purpose of interpreting this Exhibit, the following terms shall have the meanings set out below:

(a) "**Data Importer**" and "**Data Exporter**" shall have the same meaning assigned to them in **Exhibit B** (Jurisdiction Specific Terms).

(b) "**Disclosure Request**" means any request from law enforcement authority or other governmental authority with competent authority and jurisdiction over the Data Importer for disclosure of Personal Data processed under the Addendum.

(c) "**EO 12333**" means U.S. Executive Order 12333.

(d) "**FISA**" means the U.S. Foreign Intelligence Surveillance Act.

(e) "**Schrems II Judgment**" means the judgment of the European Court of Justice in Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems.

3. Applicability of Surveillance Laws to Data Importer

3.1. U.S. Surveillance Laws

(a) Data Importer represents and warrants that, as of the Effective Date, it has not received any national security orders of the type described in Paragraphs 150-202 of the Schrems II judgment.

(b) Data Importer represents that it reasonably believes that it is not eligible to be required to provide information, facilities, or assistance of any type under FISA Section 702 because:

i. No court has found Data Importer to be an entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C. § 1881(b)(4); or (ii) an entity belonging to any of the categories of entities described within that definition.

ii. If Data Importer were to be found eligible for process under FISA Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to UPSTREAM collection pursuant to FISA Section 702, as described in paragraphs 62 and 179 of the Schrems II judgment.

(c) EO 12333 does not provide the U.S. government the ability to order or demand that Data Importer provide assistance for the bulk collection of information and Data Importer shall take no action pursuant to U.S. Executive Order 12333.

3.2. **General provisions about surveillance laws applicable to Data Importer**

(a) Data Importer commits to provide, upon request, information about the laws and regulations in the destination countries of the transferred Personal Data applicable to Data Importer that would permit access by public authorities to the transferred Personal Data, in particular in the areas of intelligence, law enforcement, or administrative and regulatory supervision applicable to the transferred Personal Data. In the absence of laws governing the public authorities' access to Personal Data, Data Importer shall provide Data Exporter with information and statistics based on the experience of Data Importer or reports from various sources (such as partners, open sources, national case law, and decisions from oversight bodies) on access by public authorities to Personal Data in situations of the kind of data transfer at hand. Data Importer providing the information referred to in this subparagraph may choose the means to provide the information.

(b) Data Importer shall monitor any legal or policy developments that might lead to its inability to comply with its obligations under the Standard Contractual Clauses and this Exhibit, and promptly inform Data Exporter of any such changes and developments. When possible, Data Exporter shall inform Data Exporter of any such changes and developments ahead of their implementation.

4. Obligations on Data Importer Related to Disclosure Requests

4.1. In the event Data Importer receives a Disclosure Request, Data Importer shall:

(a) Promptly (and, when possible, before disclosing the transferred Personal Data to the public authority) notify Data Exporter of the Disclosure Request by using the contact details provided in Section 19 of the Addendum, and, where possible, the Data Subject, unless prohibited by law, or, if prohibited from notifying Data Exporter, Data Importer shall use all lawful efforts to obtain the right to waive the prohibition to communicate information relating to the Disclosure Request to Data Exporter as soon as possible. This includes, but is not limited to, informing the requesting public authority of the incompatibility of the Disclosure Request with the safeguards contained in the Standard Contractual Clauses and the resulting conflict of obligations for Data Importer and documenting this communication.

(b) Ask the public authority that issued the Disclosure Request to redirect its request to the Data Exporter to control conduct of the disclosure.

(c) Use all lawful efforts to challenge the Disclosure Request on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable EEA Member State law or any other Applicable Data Protection Law.

(d) Seek interim measures with a view to suspend the effects of the Disclosure Request until the competent court has decided on the merits.

(e) Not disclose the requested Personal Data until required to do so under the applicable procedural rules.

(f) Provide the minimum amount of information permissible when responding to the request, based on a reasonable interpretation of the request.

4.2. For the purpose of this Section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

5. Information on Requests for Personal Data by Public Authorities

5.1. Data Importer commits to provide Data Exporter with sufficiently detailed information on all requests for Personal Data by public authorities which Data Importer has received over a specified period of time (if any), in particular in the areas of intelligence, law enforcement, administrative, and regulatory supervision applicable to the transferred data and comprising information about the requests received, the data requested, the requesting body, and the legal basis for disclosure and to what extent Data Importer has disclosed the requested Personal Data. Data Importer may choose the means to provide this information.

6. Backdoors

6.1. Data Importer certifies that:

(a) It has not purposefully created backdoors or similar programming for governmental agencies that could be used to access Data Importer's systems or Personal Data subject to the Standard Contractual Clauses;

(b) It has not purposefully created or changed its business processes in a manner that facilitates government access to Personal Data or systems; and

(c) National law or government policy does not require Data Importer to create or maintain back doors or to facilitate access to Personal Data or systems.

6.2. Data Exporter will be entitled to terminate the contract on short notice in cases in which Data Importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform Data Exporter once their existence comes to its knowledge.

7. Information About Legal Prohibitions

7.1. Data Importer will provide Data Exporter information about the legal prohibitions on Data Importer to provide information under this Exhibit. Data Importer may choose the means to provide this information.

8. Additional Measures to Prevent Authorities from Accessing Personal Data

8.1. Notwithstanding the application of the security measures set forth in the Addendum, Data Importer will implement the following technical, organizational, administrative, and physical measures designed to protect the transferred Personal Data:

(a) Encryption of the transferred Personal Data in transit using the Transport Layer Security (TLS) protocol version 1.2 or higher with a minimum of 128-bit encryption;

(b) Encryption at rest within software applications used by Data Importer using a minimum of AES-256;

(c) Active monitoring and logging of network and database activity for potential security events, including intrusion;

(d) Regular scanning and monitoring of any unauthorized software applications and IT systems for vulnerabilities of Data Importer;

(e) Restriction of physical and logical access to IT systems that Process transferred Personal Data to those officially authorized persons with an identified need for such access;

(f) Firewall protection of external points of connectivity in Data Importer's network architecture;

(g) Expedited patching of known exploitable vulnerabilities in the software applications and IT systems used by Data Importer; and

(h) Internal policies establishing that:

i. Where Data Importer is prohibited by law from notifying Data Exporter or the Data Subject of a request or order from a public authority for transferred Personal Data, Data Importer shall take into account the laws of other jurisdictions and use best efforts to request that any confidentiality requirements be waived to enable it to notify the competent supervisory authorities;

ii. Data Importer must require an official, signed document issued pursuant to the applicable laws of the requesting third party before it will consider a request for access to transferred Personal Data;

iii. Data Importer's senior legal team and corporate management shall be notified upon receipt of each request or order for transferred Personal Data. ;

iv. Data Importer shall scrutinize every request for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid;

v. If Data Importer is legally required to comply with an order, it will respond as narrowly as possible to the specific request; and

vi. If Data Importer receives a request from public authorities to cooperate on a voluntary basis, Personal Data transmitted in plain text may only be provided to public authorities with the express agreement of Data Exporter.

9. Inability to Comply with this Exhibit and the Standard Contractual Clauses

9.1. If Data Importer determines that it is no longer able to comply with its contractual commitments under this Exhibit, Data Exporter can swiftly suspend the transfer of Personal Data and/or terminate the EULA.

9.2. If Data Importer determines that it is no longer able to comply with the Standard Contractual Clauses or this Exhibit, Data Importer shall return or delete the Personal Data received in reliance on the Standard Contractual Clauses. If returning or deleting the Personal Data received is not possible, Data Importer must securely encrypt the data without necessarily waiting for Data Exporter's instructions.

9.3. Data Importer shall provide the Data Exporter with sufficient indications to exercise its duty to suspend or end the transfer of Personal Data and/or terminate the contract.

10. Termination

10.1. This Exhibit shall automatically terminate with respect to the Processing of Personal Data transferred in reliance of the Standard Contractual Clauses if the European Commission or a competent regulator approves a different transfer mechanism that would be applicable to the Restricted International Transfers covered by the Standard Contractual Clauses (and, if such mechanism applies only to some of the data transfers, this Exhibit will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Exhibit.