INTERNATIONAL DATA PROCESSING ADDENDUM

With EU Standard Contractual Clauses

THIS DATA PROCESSING ADDENDUM is made **[date as designated in electronic record]**

BETWEEN

(1) System User and/or Application User: [as designated in electronic record] ("System User"); and

(2) FIA Technology Services, LLC ("**FIA Tech**").

Background

(A) FIA Tech provides services ("**FIA Tech Services**") to System User under separate agreement(s) governing the FIA Tech Services ("**Main Agreement(s)**"). In connection with the FIA Tech Services, the parties anticipate that FIA Tech may, from time to time, process Personal Data (as defined below).

(B) The System User and FIA Tech enter into this Data Processing Addendum ("**DPA**") to ensure that adequate safeguards are in place to promote the protection of Personal Data as required by the Data Protection Laws.

(C) This DPA amends any Main Agreement(s) between the parties subject to Section 9.2 below.

(D) ~~(D)~~ The European Union's ("**EU**") Standard Contractual Clauses (the "**SCC**") are attached to this DPA. ~~This DPA is broader than the SCC. Sections of this DPA may apply to Personal Data transferred under the SCC to the extent that it is a business term or a term that does not contradict the SCC.~~ Sections 9.3, 9.4, and 9.5 describe the order of precedence between the Main Agreement(s), the DPA, and the SCC in the instance of a conflict in terms.

(E) The parties intend for the SCC to apply only to transfers out of jurisdictions where the SCC are deemed to apply.

(F) This DPA consists of the following Attachments, Appendices, and Annexes:

(I) Attachment 1 Details of the Processing Activities

(II) Attachment 2 Standard Contractual Clauses (Module 2)

(III) Attachment 3 UK Addendum to the EU Commission Standard Contractual Clauses

~~(I) Attachment 1 Details of the Processing Activities~~
~~(II) Attachment 2 Sub-Processor/Covered Supplier Listing~~
~~(III) Attachment 3 Standard Contractual Clauses (Controller to Processor)~~
~~(a) Appendix 1 Designation of Exporter/Importer and Processing Operations~~
~~(b) Appendix 2 Description of the Importer's Technical and Organisational Measures~~
~~(IV) Attachment 4 Standard Contractual Clauses (Controller to Controller)~~
~~(a) Annex A Data Processing Principles~~
~~(b) Annex B Description of the Transfer~~

1. Definitions

1.1 The following expressions are used in this DPA and have these meanings (these definitions do not apply to the SCC):

(a) "**Account Data**" means the Personal Data of any individual acting on behalf of the System User ~~in connection~~shared with ~~the~~ System ~~User's account or whose Personal Data~~User which FIA Tech is ~~associated with the System User's account.~~ a Controller. Account Data does not include Customer Data;

(b) "**Customer**" means System User's account holder and any individual personally identified with the account;

(c) "**Customer Data**" means the Personal Data processed by FIA Tech on behalf of System User for purposes of providing the FIA Tech Services under the Main Agreement(s). Customer Data does not include Account Data;

(d) "**Data Subject Request**" means a request from or on behalf of a data subject relating to access to, or rectification, erasure or data portability in respect of that person's Personal Data or an objection or request to restrict from or on behalf of a data subject to the processing of that person's Personal Data;

(e) "**Data Protection Laws**" means all laws and regulations ~~as are applied~~applicable to the processing of Personal Data, including the laws of the EU, the European Economic Area ("**EEA**"), their member states ~~and the United Kingdom ("**UK**"),~~ including (where applicable) the ~~General~~GDPR (as defined below); the GDPR in such form as incorporated into the laws of the United Kingdom ("**UK**") and the UK Data Protection ~~Regulation ("~~Act 2018 (collectively "**UK GDPR**~~");~~") the laws of Australia, including the Australian Privacy Protection Act ("**APP**"); the laws of Canada, including the Federal Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), the ~~laws of Brazil ("**LGPD**~~California Consumer Privacy Act ("CCPA"), the laws of Brazil ("**LGPD**"); the Swiss Federal Act of 19

Commented [A1]: Streamlined Document Structure

June 1992 on Data Protection, the Ordinance to the Swiss Federal Act on Data Protection and the revised Swiss Federal Act of 25 September 2020 on Data Protection which comes into force on 01 January 2023 (together the "Swiss FADP"); and the data protection or privacy laws of any other country, including, without limitation, Switzerland and the Russian Federation, and any laws substantially amending, replacing or superseding any of the foregoing;

(f) **"FIA Tech Group"** means FIA Tech and any corporate entities which are from time to time under Common Control with or Control of FIA Tech;

(g) "**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 the free movement of such data (known as the General Data Protection Regulation~~);~~ or "**EU GDPR**") and the EU GDPR 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 ("**UK GDPR**");

~~(a) *"Incident" means: (a) a complaint or a request about the exercise of an individual's rights under Data Protection Laws; (b) an investigation into or seizure of Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent; or (c) a "Material Breach" of the security and/or confidentiality as set out in this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. A "Material Breach" is one that is likely to result in a significant risk to the rights and freedoms of individuals, or that would require notification to individuals or regulators under the law of the applicable jurisdiction.*~~

Commented [A2]: See Personal Data Breach

(h) "**Personal Data**" means all personal identifiable or identified information, as defined in the Data Protection Laws and to which Data Protection Laws apply, including Customer Data and Account Data.

(i) "**Processing**," "~~**Data** **Controller**~~," "**Data Subject**," "**Supervisory Authority**", "**Personal Data Breach**" and "~~**Data** **Processor**~~" shall have the meanings, or similar meanings, ascribed to them ~~in the GDPR~~under Data Protection Laws; and

(j) **"Standard Contractual Clauses"** or **"SCC"** refer to the template clauses approved by the European Commission for the transfer of Personal Data to Data Processors or Data Controllers established in third countries, in its decision 2021/914 as published by the ~~EU~~European Commission on ~~5 February 2010 and 27 December 2004, respectively,~~4 June 2021 or as the ~~EU~~European Commission may revise and re-issue. ~~These~~The SCC are integrated ~~by reference~~into this DPA and appear as Attachment ~~3 and Attachment 4~~ 2 to this DPA.

(k) An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or under an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it under its governance documents or under a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

(l) "**System User Group**" means System User and any corporate entities which are from time to time under Common Control with or Control of System User.

(m) "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner's Office, in force as of 21 March 2022. The UK Addendum is integrated into this DPA and appears as Attachment 3 to this DPA.

Commented [A3]: UK ICO March 2022 Guidance

2. Status of the Parties

2.1 Each of the System User and FIA Tech warrant in relation to Personal Data that it will ~~(and will ensure that any of its staff and/or sub-processors)~~ comply with the Data Protection Laws applicable to them and to the particular Personal Data processed by each.

2.2 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that:

(a) the System User is the ~~Data~~ Controller, as between them, with respect to Customer Data;

(b) FIA Tech is the ~~Data~~ Processor, as between them, as to Customer Data;

(c) FIA Tech is the ~~Data~~ Controller, as between them, with respect to Account Data;

(d) The parties recognize that some Personal Data may be under common control with other system users~~;~~.

~~(a) FIA Tech agrees to process Personal Data (whether Customer Data or Account Data) according to the terms of this DPA to the extent not inconsistent with the rights in Customer Data that may be controlled with another system user.~~

3. System User Obligations

3.1 With respect to all Personal Data which System User provides to FIA Tech, ~~whether it is Customer Data or Account Data~~, the System User shall have sole responsibility for the accuracy, quality, and legality of the processing and transfer of Personal Data.

(a) System User warrants that it has obtained all necessary ~~rights~~authorizations to provide to FIA Tech the Personal Data for processing in connection with the provision of the FIA Tech Services.

(b) System User understands, as a ~~Data~~ Controller, that it is responsible (as between System User and FIA Tech) for all obligations of a ~~Data~~ Controller under the Data Protection Laws, including, but not limited to:

(i) providing appropriate notification to individuals about potential cross-border transfers of Personal Data and obtaining enforceable consent if the Data Protection Laws require;

(ii) responding to requests from individuals about their Personal Data and the processing of the same, including requests to have Personal Data altered, corrected, or erased, and providing copies of the actual Personal Data processed;

(iii) notifying individuals and any relevant regulators or authorities of any ~~Incident~~Personal Data Breach as may be required by law in the relevant jurisdiction;

(iv) maintenance of the relevant processing record.

4. FIA Tech Obligations

4.1 With respect to all Personal Data processed by FIA Tech, FIA Tech agrees it shall:

(a) only process the Customer Data in order to provide FIA Tech Services and shall act only in accordance with this DPA and the System User's written instructions *which are entirely represented by the Main Agreement(s), any mutually agreed addendums thereto, this DPA and its Attachments, and the Standard Contractual Clauses, if relevant*;

(b) implement appropriate technical and ~~organisational~~organizational measures to ensure a level of security appropriate to the risks that are presented by the Processing, in particular protection against accidental or unlawful destruction, loss, alteration, ~~unauthorised~~unauthorized disclosure of, or access to Personal Data.

(c) take reasonable steps to ensure that only ~~authorised~~authorized personnel have access to such Personal Data and that any persons

whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

(d) provide the System User with reasonable cooperation and assistance in respect of ~~an Incident~~a Personal Data Breach as detailed in Section 5 below;

(e) notify the System User if it receives a Data Subject Request:

(i) To the extent System User does not have the ability to address a Data Subject Request, FIA Tech shall (upon the System User's request) provide reasonable assistance to facilitate a Data Subject Request to the extent FIA Tech is able, subject to its contractual obligations to other system users and the laws governing the Main Agreement(s).

(f) ~~(f)~~ The deletion or return of Customer Data shall be governed by the terms of the Main Agreement(s) or, if applicable, Clause 12 of the SCC; however, nothing in Clause ~~12~~8.5 of the SCC shall be interpreted to compel FIA Tech to delete or return Personal Data that is processed by another system user. FIA Tech cannot delete or return Customer Data that is associated with a record in another system user's account or where it must be retained for audit trail or other obligations to account to regulatory authorities.

(g) ~~(g)~~ FIA Tech will provide such assistance as the System User reasonably requests (taking into account the nature of processing and the information available to FIA Tech) with respect to accounting for and documenting System User's compliance with its obligations under relevant Data Protection Laws. At a minimum, upon written request, FIA Tech will produce to System User a copy of any third-party audit reports concerning the adequacy of FIA Tech's technical security measures.

(h) With respect to the Personal Data of individuals with rights under the Data Protection Laws of the ~~EU,~~ EEA, UK or Switzerland, refrain from disclosing Personal Data to any third party, including, but not limited to, relevant legal authorities, until a court with competent jurisdiction over the data importer requires such disclosure.

~~Incident~~5. Personal Data Breach Management

5.1 When ~~either party~~FIA Tech becomes aware of ~~an Incident~~a Personal Data Breach affecting Customer Data, it shall ~~promptly~~, without undue delay, notify the ~~other~~System User about the ~~Incident~~Personal Data Breach and shall ~~reasonably cooperate in order~~provide reasonable cooperation and assistance to the System User to enable the ~~other party~~System User to understand the ~~Incident, to formulate a correct response,~~Personal Data Breach and to take suitable further steps in respect of the ~~Incident.~~Personal Data Breach.

~~2.2 Both parties shall at all times have in place written procedures which enable them to promptly respond to the other about an Incident. Where the Incident is reasonably likely to require a data breach notification under applicable laws, the party responsible for the Incident shall notify the other no later than 24 hours after having become aware of the Incident.~~

5.2 When System User becomes aware of a Personal Data Breach affecting Account Data, it shall, without undue delay, notify FIA Tech about the Personal Data Breach and shall provide reasonable cooperation and assistance to FIA Tech to enable FIA Tech to understand the Personal Data Breach and to take suitable further steps in respect of the Personal Data Breach.

6. Sub-Processing

6.1 The System User grants a general authorization to FIA Tech and other members of the FIA Tech Group to appoint: (a) other members of the FIA Tech Group as sub-processors; and (b) any third-party identified in Attachment 2 as a sub-processor.

6.2 FIA Tech will maintain a list of sub-processors (which can be accessed at https://fia-tech.com/subprocessors-covered-suppliers/) and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of ~~Personal~~Customer Data.

6.3 FIA Tech will ensure that any sub-processor it engages to provide services on its behalf does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on FIA Tech in this DPA or as may be required in the SCC.

7. Cross-Border Data Transfers

Commented [A4]: UK GDPR, Swiss FADP

7.1 The System User acknowledges that the provision of the FIA Tech Services under the Main Agreement(s) will require the processing of ~~Personal Data by FIA Tech and sub-processors in countries outside the EEA.~~Customer Data by FIA Tech and sub-processors in countries outside the EEA, Switzerland and the UK, in particular in the United States. To the extent an adequate transfer safeguard is required for the transfer of Customer Data from the System User to FIA Tech by data protection laws in the EEA and Switzerland, as confirmed by relevant competent authorities, the System User and FIA Tech enter into and agree to bound by the provisions of Module 2 of the Standard Contractual Clauses set out in Attachment 2 in relation to such transfers of Customer Data.

~~2.3 The parties agree to adopt the SCC if Personal Data is expected to be transferred from a jurisdiction where the SCC are deemed to apply.~~

~~2.4 The System User will provide appropriate notification about potential cross-border transfers of Personal Data to relevant individuals whose Personal Data may be subject to such a transfer(s) and obtain enforceable consent if the Data Protection Laws require.~~

7.2 To the extent an adequate transfer safeguard is required for the transfer of Customer Data subject to the Swiss FADP, from System User to FIA Tech in the United States, by Swiss data protection laws, as confirmed by relevant competent authorities, the System User and FIA Tech enter into and agree to be bound by the provisions of the Standard Contractual Clauses set out in Attachment 2 ("Swiss Standard Contractual Clauses") in relation to such transfers of Customer Data. For the purposes of the Swiss Standard Contractual Clauses any references to EU legislation, EU authorities and the EU Member States in the Swiss Standard Contractual Clauses are amended to reflect corresponding Swiss legislation, Swiss competent authorities as appropriate, including the following amends:

(a) The following definitions are included in the EU Standard Contractual Clauses prior to Section 1 of the EU Standard Contractual Clauses: (i) "Swiss FADP": the Swiss Federal Act of 19 June 1992 on Data Protection, the Ordinance to the Swiss Federal Act on Data Protection and the revised Swiss Federal Act of 25 September 2020 on Data Protection which comes into force on 01 January 2023; and (ii) "the Switzerland Data Protection Laws": All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in Switzerland, including the Swiss FADP;

(b) References to "Regulation (EU) 2016/679" OR "That Regulation" are replaced by "Switzerland Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of Swiss Data Protection Laws;

(c) References to Regulation (EU) 2018/1725 are removed;

(d) References to the "Union", "EU" and "EU Member State" are all replaced with "Switzerland";

(e) The Supervisory Authority selected for the purposes of Clause 13 (Supervision) of the Swiss Standard Contractual Clauses is the Swiss Federal Data Protection and Information Commissioner (FDPIC).

(f) Clause 17 (Governing law) of the Swiss Standard Contractual Clauses shall refer to the laws of Switzerland as the governing law of the Swiss Standard Contractual Clauses and Clause 18 (Choice of forum and jurisdiction) shall refer to the Swiss courts as the proper forum and jurisdiction for disputes and legal proceedings arising under the Swiss Standard Contractual Clauses.

7.3 To the extent an adequate transfer safeguard is required for the transfer of Customer Data subject to the UK GDPR, from System User to FIA Tech in the United States, by UK data protection laws, as confirmed by relevant competent authorities, the System User and FIA Tech enter into and agree to be bound by the provisions of the Standard Contractual Clauses set out in Attachment 2,

complemented by the UK Addendum as set out in Attachment 3 in relation to such transfers of Customer Data.

7.4 FIA Tech shall ensure that any onward transfers of Customer Data to sub-processors outside the EEA and UK will be compliant with Data Protection Laws.

8. Liability

8.1 Subject to the limitations of liability in the Main Agreement(s), each party shall be liable to the other for damages it causes by any breach of this DPA. Liability as between the parties is limited to actual damage suffered. Punitive damages are specifically excluded.

9. General

9.1 If the System User determines that ~~an Incident~~a Personal Data Breach must be reported to any regulator or enforcement authority, and/or Data Subjects, and/or the public or portions of the public, the System User will notify FIA Tech before the report is made and supply FIA Tech with copies of any written documentation to be filed with the authorities and of any notification the System User proposes to make (whether to any regulator or enforcement authority, and/or Data Subjects, and/or the public or portions of the public) which references FIA Tech, its security measures and/or role in the ~~Incident~~Personal Data Breach, whether or not by name. Subject to the System User's compliance with any mandatory notification deadlines under the Data Protection Laws, the System User will consult with FIA Tech in good faith and take account of any clarifications or corrections FIA Tech reasonably requests to such notifications and which are consistent with the Data Protection Laws.

9.2 This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement(s), which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement(s), the terms of this DPA shall prevail, but only so far as the subject matter concerns the processing of ~~Personal~~Customer Data.

9.3 Except to the extent that the SCC differ, FIA Tech's liability to the System User and to each member of the System User Group (taken together) under or in connection with this DPA shall be subject to the same limitations and exclusions of liability as apply under the Main Agreement(s) as if that liability arose under the Main Agreement(s).

9.4 Except to the extent permitted in connection with FIA Tech's obligations under the SCC, no third person or entity has the right to enforce this DPA.

9.5 With respect to transferred, GDPR-protected Personal Data only, the SCC shall take precedence over any explicitly contradictory term in the DPA or Main Agreement(s). The Main Agreement(s) and the DPA shall take precedence when the SCC is silent on a term.

9.6 This DPA and the SCC set out all of the terms that have been agreed between the parties in relation to the subjects covered by it and supersede any other agreements or terms between the individual and/or legal entity agreeing to these terms and FIA Tech. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA.

9.7 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 shall be either (i) amended as necessary to ensure its 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 had never been contained therein.

9.8 This DPA shall be governed by and construed in accordance with the laws of the country or territory stipulated for this purpose in the Main Agreement(s) and each party agrees to submit to the choice of jurisdiction as stipulated in the Main Agreement(s) in respect of any claim or matter arising under this DPA.

9.9 The SCC are governed by the law of the member state indicated in the SCC.

9.10 The signatories hereto warrant and represent that they are duly authorized to bind the respective party, and to execute this DPA and all Attachments, Appendices, and Annexes hereto.

EXECUTED by and on behalf of~~:~~
FIA Technology Services, ~~Inc.~~LLC

Signature: …….

Name: Nick Solinger

Title: ~~President &~~ CEO

EXECUTED electronically by and on behalf of **[the individual and/or legal entity as designated in the electronic record]**:

Signature: …….

Name: **[As designated in the electronic record]**

Title: **[As designated in the electronic record]**

Attachment 1

Details of the Processing Activities

Written Instructions:

The Main Agreement(s) constitute System User's written instructions.

Subject matter and duration of the Processing of Personal Data:

The subject matter and duration of the Processing of Personal Data are set out in the Main Agreement(s).

The nature and purpose of the Processing of Personal Data:

The nature and purpose of the Processing of Personal Data are set out in the Main Agreement(s).

The type of Personal Data:

FIA Tech processes the following types of Customer Data, depending on the FIA Tech Services being used by System User:

i. **Contact Information:** given name, surname, maiden name, middle name, birth name, or any additional names, preferred salutation, alias, personal and/or business address, title, personal and/or business phone number (including, but not limited to, mobile phone number), personal and/or business fax number, personal and/or business email address, or other contact information.

ii. **Signatures.**

iii. **Employment Information:** country of residence and/or employment, city of residence and/or employment, occupation, employer, employment status, or other identity or occupation-related data.

iv. **Identifiers:** account number, Tag50 or other trading identifier, usernames or other identifying numbers or references.

v. **Financial Details**: bank account related information or other financial details.

vi. **Meeting Data**: schedules, calendar invites, attendance notes or other types of communication, call or meeting data.

vii. **Voice Recordings**.

viii. **Digital Identifiers**: IP address, browser-generated information, device information, geo-location markers, and other digital identifiers used for purposes including, but not limited to, tracking, profiling or identifying location

ix. **Permissioning:** data relating to role or access rights in FIA Tech's system or other similar information.

~~x. **Monitoring Data:** ongoing monitoring data in connection with compliance, fraud prevention, security, and system use, or other monitoring data.~~

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

The categories of Data Subject may include some or all of the following:

1. System ~~User Representative –~~ User's, and System User's ~~and it's affiliates'~~ affiliate's, representatives (including, employees, officers, directors, partners, ~~affiliates,~~ owners, consultants, ~~vendors~~ vendor representatives, contractors and ~~agents.~~ agent representatives).

2. Client or Counterparty Representative – System User's or it's affiliates' client's (and each of such client's respective client's) or counterparty's employees, officers, directors, partners, affiliates, owners, consultants, vendors, contractors and agents.

The obligations and rights of System User

The obligations and rights of System User are set out in the Main Agreement(s) and in this DPA.

Attachment 2

~~**Sub-Processor/Covered Supplier Listing**~~

Commented [A5]: Moved to Annex III

STANDARD CONTRACTUAL CLAUSES (Module 2)

This Schedule 1 is part of and subject to the terms of the Agreement.

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: **[As designated in the electronic record]**

Address: **As and if on file**

(the data **exporter**)

And

Name of the data importing organization: FIA Technology Services, LLC

Address: 2001 K St NW, Suite 730 North Tower, Washington DC 20006

(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~~

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into

account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of

noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 60 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[1] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually

[1] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter withRegulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[1];

[1] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to

suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State which the System User is located.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Member State which the System User is located.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

~~Attachment 3~~

~~Standard Contractual Clauses (Controller to Processor)~~

~~Appendix 1 to Attachment 3~~

~~Designation of Exporter/Importer and Processing Operations~~

Commented [A6]: Existing Attachment III replaced in its entirety.

Standard Contractual Clauses Moved to Attachment II

UK Addendum now located in Attachment III

Commented [A7]: See Attachment I Details of Processing Activities

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: System User as defined in the DPA

Address: System User's address detailed in the DPA.

Contact person's details: as and if on file within "Agreements and Protocols" section of Accelerate platform, or as designated below:

Activities relevant to the data transferred under these Clauses:

Data exporter uses integrated cloud-based systems and web-based platforms offered by data importer to digitally manage legal agreements (give-up agreements, etc.) and the structured and unstructured data involved in those agreements, settle brokerage, automate reconciliations, and invoice data management, manage risk, meet regulatory compliance requirements, and obtain other trade processing services and reference data products required across the pre- and post-trade space.

Signature: …….

Date: **[As designated in the electronic record]**

Role: Controller

Data importer(s):

Name: FIA Technology Services, LLC

Address: 2001 K Street NW, Suite 730 – North Tower
Washington DC 20006

Contact person's name, position, and contact details:

NAME: Rebekah Metz
POSITION: VP, Operations
PHONE/EMAIL: fiatech-privacy@fia-tech.com

Activities relevant to the data transferred under these Clauses:

Data importer provides integrated cloud-based systems and web-based platforms for its clients to digitally manage legal agreements (give-up agreements, etc.) and the structured and unstructured data involved in those agreements, settle brokerage, automate reconciliations and invoice data management, manage risk, meet regulatory compliance requirements, as well as other trade processing services and reference data products required across the pre- and post-trade space.

Signature: .....

Date: **[As designated in the electronic record]**

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

The Personal Data transferred concern the categories of Data Subjects detailed in Attachment 1 to the DPA.

Categories of personal data transferred:

The Personal Data transferred concern the categories of Personal Data detailed in Attachment 1 the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Categories of sensitive data will not be transferred under this DPA.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

The transfer takes place on a continuous basis under the terms of the Main Agreement.

Nature of the processing:

The nature of the Processing will be for the data importer to provide FIA Tech Services to the data exporter pursuant to the terms of the Main Agreement.

Purpose(s) of the data transfer and further processing:

The objective of Processing of Personal Data by data importer is the performance of the FIA Tech Services. The Personal Data will be subject to the following Processing operations: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The Personal Data will be retained by the data importer for the duration of the FIA Tech Services.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Sub-processor information can be accessed at https://fia-tech.com/subprocessors-covered-suppliers/

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

The applicable supervisory authority based in the jurisdiction where the System User is located.

~~**Appendix 2 to Attachment 3**~~

~~**Description of the Importer's Technical and Organisational Measures**~~

~~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):**~~

~~This Appendix relates to the FIA Tech Services and the Customer Data that FIA Tech processes related thereto.~~

Commented [A8]: See ANNEX II

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Information Security Organization

FIA Tech maintains a risk and information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the type of Customer Data that FIA Tech processes; and (b) the need for security and confidentiality of such Customer Data. FIA Tech's security program is designed to:

- Protect confidentiality, integrity, and availability of Customer Data in FIA Tech's possession or control or to which FIA Tech has access;
- Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data; and
- Safeguard Customer Data as set forth in any applicable law.

Please refer to the FIA Tech Information Security Policy for additional details of the administrative, technical, and operational safeguards within FIA Tech's security program. The current version of the FIA Tech Information Security Policy is available by request from Client Services. Without limiting the generality of the foregoing, FIA Tech's security program includes:

1. **Risk & Information Security Responsibility**
   The Head of Risk & Information Security is responsible for the development, implementation, and maintenance of the risk & information security program. Members of the FIA Tech senior management team are involved in risk-related discussions and the Head of Risk & Information Security reports directly to the FIA Tech President / CEO.

2. **Security Training and Awareness**

Promoting a culture of security awareness is the cornerstone of human resources security. All personnel are required to undergo periodic risk training for the purpose of evaluating the existing risk profile, changing behavior, and reducing the overall risk exposure. Graded, post-training exercises (with associated feedback) are an integrated part of the risk & information security program.

3. **Access Control**
   Access to applications and other sensitive systems containing Customer Data is role-based with application of the principle of separation of duties. The concept of *'least privilege'* is a centerpiece of the access control process. Additional controls include processes to ensure the timely removal of access in the event of leaving the firm or an internal job or responsibility change. Regular access reviews are performed on all systems to ensure alignment with best industry practices.

4. **Physical Security**
   Controls are in place to provide reasonable assurance that physical access to the network infrastructure associated with Customer Data is limited to authorized individuals. These controls include the timely removal of all physical access when employees leave the company. Additionally, proper environment controls are in place to assure the integrity and sustainability of Customer Data.

5. **Data Security**
   All data containing Customer Data is protected and secured with controls aligned with best industry practices. These controls include, but may not be limited to: encryption in transit and at rest, measures to protect the integrity and availability of the data, secure end-of-life disposal of physical servers and other tangible property associated with Customer Data.

6. **Network Security**
   All networks hosting Customer Data are protected with controls aligned with industry best practices. These controls include, but may not be limited to: log file security and monitoring, firewalls, intrusion detection systems, endpoint security, and external penetration testing by an independent third party.

7. **Application Security**
   All applications are developed according to best industry practices and specifically guided by internal standards and policies. These include, but may not be limited to: separate application environments, security code scanning, open source code scanning and application penetration testing.

8. **Change Management**
   Controls and processes are in place to ensure that all changes made to production systems, applications, networks, and other critical infrastructure associated with Customer Data are aligned with best industry practices. This includes, but may not be limited to: processes for documenting, testing, and approving normal maintenance changes, upgrades, fixes and vulnerability patching.

9. **Penetration Testing**

All applications and networks associated with Customer Data undergo regular penetration testing by an independent third party. This testing uses highly specialized tools, custom testing setups, and ethical hacking techniques to identify any existing security gaps.

10. Business Continuity Program ("BCP") & Pandemic Planning

A comprehensive BCP is in place to ensure that FIA Tech can respond to all types of business interruptions (*e.g.*, loss of facilities, loss of people, loss of technology, loss of utilities, pandemic, etc.) in a timely and efficient manner.

11. Incident Response

An incident response plan exists to ensure a timely and proper response to a risk or information security related event associated with Customer Data.

12. Risk Monitoring

Risk monitoring controls are in place to provide assurance that existing policies and processes are being followed. These controls include, but may not be limited to: log file security and alerting, network security alerting, BCP and disaster recovery testing, and the monitoring of employee training.

13. Program Adjustments

FIA Tech actively monitors, evaluates, and adjusts its risk and information security processes, taking into account changes in or to: (1) the threat landscape; (2) its business environment; (3) applicable technology; and (4) legal, regulatory, or other requirements.

ANNEX III – LIST OF SUB-PROCESSORS

The list of Sub-processors can be accessed at https://fia-tech.com/subprocessors-covered-suppliers/.

Attachment 3

UK Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start date	The date of the Main Agreement and the DPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	The System User as defined in the DPA	Full legal name: FIA Technology Services, LLC Trading name (if different): N/A Main address (if a company registered address): 2001 K Street NW, Suite 730 – North Tower, Washington DC 20006, USA
Key Contact	See Annex I to the SCC	See Annex I to the SCC
Signature (if required for the purposes of Section 2)	**EXECUTED** electronically by and on behalf of **[the individual and/or legal entity as designated in the electronic record]**: ……	……

Formatted: Not Highlight

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: The date of the Main Agreement and the DPA. Reference (if any): SCC Other identifier (if any):N/A

	Module 2: Module in Operation Clause 7 (Docking Clause): No Clause 11 (Option): No Clause 9a: General Authorisation Clause 9a: 60 day Time Period

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex I to the Approved EU SCCs
Annex 1B: Description of Transfer: See Annex I to the Approved EU SCCs
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II to the Approved EU SCCs
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III to the Approved EU SCCs

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising

from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority~~/~~" and "supervisory authority" ~~shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority"~~are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall ~~mean the competent data protection authority in the territory in which~~be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter ~~is established);~~and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with ~~the laws applicable to the data exporter.~~

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

~~Attachment 4~~

Commented [A9]: Attachment IV removed.

Standard Contractual Clauses Moved to Attachment II