Global Tax Network

JURISDICTION SPECIFIC TERMS

Relating to the GTN Data Processing Addendum

These Jurisdiction-Specific Terms are an integral part of the GTN DATA PROCESSING ADDENDUM ("Addendum"). Capitalized terms which are used but not defined in this document shall have the meaning given to those terms in the Addendum. By signing the Addendum, the Parties have agreed to comply with these Jurisdiction-Specific Terms which apply to the extent that the Parties Process Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions identified herein.

1. EEA

a) Definitions.

i. "EEA" means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.

ii. "EEA Data Protection Laws" means the GDPR and all laws and regulations of the EEA (as defined above), applicable to the Processing of Personal Data.

iii. "EU 2021 Standard Contractual Clauses" (as used in these Jurisdiction-Specific Terms) 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.

iv. "EEA Restricted Transfer" means any transfer of Personal Data subject to the EEA Data Protection Laws, 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).

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

vi. "Third Country" means a country outside of the EEA.

b) **Joint Controllership Representation and Warranties.** Each Party, when acting as a Joint Controller together with the other Party, warrants and covenants that:

i. it has determined its respective responsibilities for compliance with its obligations under the Applicable Data Protection Laws and has documented such responsibilities in writing, within the Addendum. When making such determinations, the Parties have considered, without limitation, the following:

a. implementation of general data protection principles, which is described in the Addendum;

b. legal bases for the Processing, which are described in each Party's respective privacy notice;

c. implementation of data security measures, which are described in Section 7 and Section 9 of the Addendum;

d. notification of Personal Data Breaches to the competent Supervisory Authority and to the Data Subject(s), which is described in Section 9 of the Addendum;

e. obligation to conduct data protection impact assessments, where applicable, as described in Section b)(iii) of these Jurisdiction-Specific Terms;

f. the use of a Data Processor, which is described in Section 10 of the Addendum;

g. obligation to ensure compliance with the requirements for transfers of Personal Data to Third Countries; and

h. organization of contact with Data Subjects and Supervisory Authorities, which is described in Sections 8 and 9 of the Addendum;

ii. it has determined its respective responsibilities *vis-a-vis* Data Subject(s), including without limitation, the responsibility to respond to requests when Data Subjects exercise their rights granted by Applicable Data Protection Laws and to provide information to Data Subjects as required by Applicable Data Protection Laws, taking into account the circumstances of each specific Processing situation (including which Party is competent and in a position to effectively ensure Data Subjects' rights as well as to comply with the relevant obligations under the EEA Data Protection Laws), and, where necessary, will duly communicate such information to the respective other Data Controller in the Joint Controllership context as further described in Sections 8 and 9 of the Addendum;

iii. when any proposed Processing to be carried out by the Party is likely to result in a high risk to the rights and freedoms of natural persons, it will conduct a data protection impact assessment as may be required by Applicable Data Protection Laws;

iv. Data Subjects may exercise their rights under Applicable Data Protection Laws in respect of and against each of the Data Controllers. Each Data Controller in the Joint Controllership context will proactively, without having been requested to do so, provide all due assistance and information to the respective other Data Controller in the Joint Controllership context, including but not limited to forwarding requests lodged by Data Subjects to exercise their rights under Applicable Data Protection Laws;

v. where a conflict of competence occurs with regard to a specific set of Processing operations in the Joint Controllership context, each Data Controller shall act in good faith to communicate and resolve the said conflict with the other respective Data Controller in an amicable manner, by considering and respecting, firstly, the interests and rights of the respective Data Subject(s), and, secondly, the mutual interest of both Parties, so as to avoid

joint and several liability, where the Parties fail to respect the rights of a Data Subject(s) because of an unresolved conflict of competence;

vi. it will make the essence of the Addendum available to Data Subjects as may be required by Applicable Data Protection Laws. The essence of the Addendum as it pertains to Data Subjects will include all the elements of the information required to be provided to Data Subjects under the Applicable Data Protection Laws, and in respect of each element, an indication of which joint Data Controller is responsible for ensuring compliance with the element. The essence of the arrangement shall also indicate the contact point for Data Subjects, as described in Section 16 of the Addendum; and

vii. it has identified an appropriate legal basis for the Processing under the Applicable Data Protection Laws and, where necessary, it has obtained valid consent from the relevant Data Subject(s) as defined under the Applicable Data Protection Laws to Process Personal Data of each Data Subject.

c) With regard to any EEA Restricted Transfer subject to EEA Data Protection Laws from one Party to another within the scope of the Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. a valid adequacy decision adopted by the European Commission on the basis of Article 45 of the GDPR;

ii. the Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the EEA Data Protection Laws, as the case may be); or

iii. any other lawful data transfer mechanism, as laid down in the EEA Data Protection Laws, as the case may be.

d) EU 2021 Standard Contractual Clauses

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

ii. The Parties agree that any references to sections, annexures, exhibits, modules and choices within the EU 2021 Standard Contractual Clauses as set out in this Section of these Jurisdiction Specific Terms, shall be deemed to be the same as the cognate and corresponding references to sections, annexures, exhibits, modules and choices within any appropriate, updated Standard Contractual Clauses as may be applicable from time to time pursuant to the Addendum.

iii. The Parties agree that the following modules apply:

a. Module one of the EU 2021 Standard Contractual Clauses when, in accordance with Section 4 of the Addendum, either Party is the Data Exporter or Data Importer, and acts as the Controller.

b. Module two of the EU 2021 Standard Contractual Clauses when, in accordance with Section 12 of the Addendum, the Data Exporter is Client and acts as a Controller, and the Data Importer is GTN acting as a Processor.

c. Module four of the EU 2021 Standard Contractual Clauses when, in accordance with Section 12 of the Addendum, the Data Exporter is GTN and acts as a Processor, and Data Importer is Client acting as a Controller.

iv. For the purposes of the annexures to the EU 2021 Standard Contractual Clauses and any substantially similar Standard Contractual Clauses which may be adopted by the relevant authorities in the future:

a. Annex I(A): The content of Annex I(A) is set forth in Exhibit A of the Addendum and/or Section 2 of the Processor Services Terms, as applicable.

b. Annex I(B): The content of Annex I(B) is set forth in Exhibit A of the Addendum and/or Section 2 of the Processor Services Terms, as applicable.

c. Annex I(C): The content of Annex I(C) is set forth in Section 1.d)v.c of these Jurisdiction Specific Terms and in Exhibit A of the Addendum.

d. Annex II: Refer to Appendix 1 to these Jurisdiction-Specific Terms. Where GTN is the Data Importer, its additional measures are described at https://www.gtn.com/privacy-security. Where Client is the Data Importer, it shall provide GTN with a list of its technical and organizational measures that apply in addition to the measures listed in Appendix 1.

v. Parties' Choices under the EU 2021 Standard Contractual Clauses:

a. With respect to Clause 7 of the EU 2021 Standard Contractual Clauses, the Parties choose not to include the optional docking clause.

b. With respect to Clause 9(a) of the EU 2021 Standard Contractual Clauses (when applicable), the Parties select "Option 2 – General Written Authorization" with a time period of [14 days].

c. For the purpose of Annex I.C and with respect to Clause 13 (when applicable) of the EU 2021 Standard Contractual Clauses, the Supervisory Authority is the Data Protection Commission of the Republic of Ireland.

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

e. 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.

e) In cases where the EU 2021 Standard Contractual Clauses apply, the Parties will comply with the supplemental clauses set out in Appendix 1 hereto.

f) 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 control with regard to the EEA Restricted Transfer in question.

g) The details of Processing that apply to the circumstances in which GTN acts as a Data Processor (as described in Section 12 of the Addendum) are set out in the Processor Services Data Processing Terms.

2. California

a) Definitions.

i. For the purpose of interpreting the Addendum and these Jurisdiction-Specific Terms, the following terms shall have the meanings set out below:

a. "California Data Protection Laws" includes the California Consumer Privacy Act of 2018, the California Consumer Privacy Act Regulations, and the California Privacy Rights Act of 2020, as may be amended from time to time.

b. The terms "Business Purpose", "Commercial Purpose", "Sale", "Sell", and "Share", along with their corresponding terms, whether capitalized or not, shall have the same meaning as in the California Data Protection Laws, and their related terms shall be construed accordingly.

ii. For the purpose of interpreting the Addendum and these Jurisdiction-Specific Terms, the following terms shall be interpreted as follows:

a. "Controller" includes "Business" as defined under the California Data Protection Laws.

b. "Data Subject" includes "Consumer" as defined under the California Data Protection Laws.

c. "Personal Data" includes "Personal Information" as defined under the California Data Protection Laws.

d. "Personal Data Breach" includes "Breach of the Security of the System" as defined under paragraph (g) of Section 1798.82. of the California Civil Code.

e. "Processor" includes "Service Provider" as defined under the California Data Protection Laws.;

b) Processors. Each Party shall refrain from taking any action that would cause any disclosures of Personal Data to a Data Processor to qualify as a sale of Personal Data. For the sake of clarity, when Processing Personal Data that is regulated by the California Data Protection Laws, each Party shall only engage a Data Processor to Process the Personal Data on its behalf for lawful and valid Business Purposes.

c) Where GTN acts as a Service Provider (as described in Section 12 of the Addendum), Client discloses Personal Data to GTN solely for: (i) valid Business Purposes; and (ii) to enable GTN to

perform the services under the Services Agreement or Business Relationship, as the case may be. GTN shall not: (i) Sell or Share Personal Data; (ii) retain, use, or disclose Personal Data for a Commercial Purpose other than providing the Processor Services or as otherwise permitted by the California Data Protection Laws; nor (iii) retain, use, or disclose Personal Data except where permitted under the Services Agreement or Business Relationship between Client and GTN. GTN certifies that it understands these restrictions and will comply with them.

3. Canada

a) When applicable, the Processing of Personal Data shall be compliant with the Canadian Federal Personal Information Protection and Electronic Documents Act and any other applicable Canadian privacy or data protection laws.

b) Client confirms that is has obtained a valid consent (as defined under PIPEDA), where necessary to Process Personal Data of each Data Subject.

4. Switzerland

a) Definitions.

i. For the purpose of interpreting the Addendum and these Jurisdiction-Specific Terms, the following terms shall have the meanings set out below:

a. "FDPIC" (as used in this Section) means the Swiss Federal Data Protection and Information Commissioner.

b. "Swiss Data Protection Laws" (as used in this Section) includes the Federal Act on Data Protection of 19 June 1992 ("FADP") and the Ordinance to the Federal Act on Data Protection.

b) Restricted Transfers. With regard to any Restricted Transfer subject to Swiss Data Protection Laws from one Party to another within the scope of the Addendum and these Jurisdiction-Specific Terms, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. 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 FDPIC of states that provide an adequate level of protection for Personal Data within the meaning of the FADP;

ii. the Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the Swiss Data Protection Laws, as the case may be); or

iii. any other lawful transfer mechanism, as laid down in Swiss Data Protection Laws, as the case may be.

c) Standard Contractual Clauses:

i. The Addendum hereby incorporates by reference the Standard Contractual Clauses, which have been adopted for use by the FDPIC with certain modifications. The Parties are deemed

to have accepted, executed, and signed the Standard Contractual Clauses where necessary in their entirety (including the annexures thereto).

ii. The Parties incorporate and adopt the Standard Contractual Clauses for Restricted Transfers subject to Swiss Data Protection Laws in the same manner set forth in Section 1.d) of these Jurisdiction Specific Terms, subject to the following:

a. Clause 13 (Annex I.C): The Supervisory Authority shall be the FDPIC. Nothing about the Parties' designation of the competent Supervisory Authority shall be interpreted to preclude Data Subjects in Switzerland from applying to the FDPIC for relief.

b. Clause 18: The Parties' selection of forum may not be construed as forbidding Data Subjects habitually resident in Switzerland from suing for their rights in Switzerland.

c. References to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the FADP and the equivalent articles or sections therein, insofar as there any Restricted Transfers subject to Swiss Data Protection Laws.

d. The Standard Contractual Clauses also protect the data of legal entities until the entry into force of the revised FADP.

iii. In cases where the Standard Contractual Clauses apply and there is a conflict between the terms of this Addendum and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail with regard to the Restricted Transfer in question.

5. United Kingdom (UK)

a) Definitions.

For the purpose of interpreting the Addendum and these Jurisdiction-Specific Terms, the following terms shall have the meanings set out below:

i. "UK Data Protection Laws" includes the Data Protection Act 2018 and the UK GDPR (as defined below).

ii. "UK GDPR" 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.

iii. "UK IDTA" means the International Data Transfer Agreement issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.

iv. "UK Restricted Transfer" includes any transfer of Personal Data (including data storage in foreign servers) subject to UK Data Protection Laws to a third country outside of the UK or an international organization.

b) UK Restricted Transfers. With regard to any UK Restricted Transfer from one Party to another within the scope of the Addendum and these Jurisdiction-Specific Terms, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. a valid adequacy decision adopted pursuant to Article 45 of the UK GDPR;

ii. the UK IDTA; or

iii. any other lawful transfer mechanism, as laid down in the UK Data Protection Laws, as the case may be.

c) UK IDTA:

i. The Addendum hereby incorporates by reference the UK IDTA. The Parties are deemed to have accepted, executed, and signed the UK IDTA where necessary in its entirety.

ii. For the purposes of the tables to the UK IDTA:

a. Table 1: The information required by Table 1 appears within Exhibit A of the Addendum and/or Section 2 of the Processor Services Terms, as applicable.

b. Table 2:

I. The UK IDTA shall be governed by the laws of England and Wales.

II. The Parties agree that any dispute arising from the UK IDTA shall be resolved by the courts of England and Wales.

III. The Parties' controllership and data transfer roles are set out in the Addendum.

IV. The UK GDPR may apply to the Data Importer's Processing of Personal Data.

V. These Jurisdiction-Specific Terms, the Addendum, and the Services Agreement or Business Relationship between the Parties, set out the instructions for Processing Personal Data.

VI. The Data Importer shall Process Personal Data for the time period set out in Exhibit A of the Addendum and/or Section 2 of the Processor Services Terms, as the case may be. The Parties agree that neither Party may terminate the UK IDTA before the end of such time period.

VII. In the Joint Controllership context, the Data Importer may transfer the Transferred Data (as defined in the UK IDTA) to another organisation or person in accordance with Section 16.1 of the UK IDTA. Where the Data Importer is GTN and is acting as a Processor, the Data Importer may only transfer Personal Data to authorized sub-Processors (if applicable), as set out within Section 10 of the Addendum read with the Processor Services Terms, or to such third parties that the Data Exporter authorizes in writing.

VIII. Each Party must review these Jurisdiction-Specific Terms and the Addendum at regular intervals, to ensure that they remain accurate and up to date and continue to provide appropriate safeguards for the Personal Data. Each Party will carry out such a review at least once each year.

c. Table 3: The content of Table 3 is set forth in Exhibit A of the Addendum and/or Section 2 of the Processor Services Terms, as the case may be, and may be updated in accordance with the Addendum.

d. Table 4: Refer to Appendix 1 to these Jurisdiction-Specific Terms. Where GTN is the Data Importer, its additional measures are described at https://www.gtn.com/privacy-security. Where Client is the Data Importer, it shall provide GTN with a list of its technical and organizational measures that apply in addition to the measures listed in Appendix 1.

e. Part 2 (Extra Protection Clauses) and Part 3 (Commercial Clauses) of the UK IDTA are noted throughout the Addendum and Services Agreement where applicable.

iii. These Jurisdiction-Specific Terms and the Addendum supplement the UK IDTA.

iv. In cases where the UK IDTA applies and there is a conflict between these Jurisdiction-Specific Terms, the Addendum, and the UK IDTA, the terms of the UK IDTA will prevail.

APPENDIX 1 TO THE JURISDICTION-SPECIFIC TERMS

Supplemental Clauses to the Standard Contractual Clauses

By this **Appendix 1** (this "Appendix"), the Parties provide additional safeguards and redress to the Data Subjects whose Personal Data is transferred pursuant to Standard Contractual Clauses. This Appendix 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 Transfer.

1. **Definitions.**

   a) "Data Importer" and "Data Exporter" shall have the same meaning assigned to them in Exhibit A of the Addendum.

   b) "EO 12333" means the U.S. Executive Order 12333**.**

   c) "FISA" means the U.S. Foreign Intelligence Surveillance Act.

   d) "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.

2. **Applicability of Surveillance Laws to Data Importer and its Data Processors.**

   a) Data Importer represents and warrants that, as of the date of the Addendum, it has not received any national security orders of the type described in Paragraphs 150-202 of 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 legal process issued under FISA Section 702: (i) an "electronic communication Data Importer" 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 legal 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 EO 12333.

3. **Backdoors**

   a) Data Importer certifies that:

      i. 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;

ii. it has not purposefully created or changed its business processes in a manner that facilitates governmental access to Personal Data or systems; and

iii. that national law or government policy applicable to Data Importer does not require Data Importer to create or maintain backdoors or to facilitate access to Personal Data or systems.

b) Data Exporter will be entitled to terminate the contract on short notice in those cases in which Data Importer does not reveal the existence of a backdoor 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.

4. **Information About Legal Prohibitions.**

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

5. **Additional Measures to Prevent Authorities from Accessing Personal Data.** Notwithstanding the application of the security measures set forth in the Addendum and in Appendix 2 to these Jurisdiction-Specific Terms, Data Importer will implement the following technical, organizational, administrative and physical measures designed to protect any the transferred Personal Data from unauthorized disclosure and access:

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 the Data Importer's software applications 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 authored software applications and IT systems for vulnerabilities of the 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; and

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

h) Internal policies establishing that 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.

i) Data Importer's Data Protection Officer shall be notified upon receipt of each request or order for transferred Personal Data.

j) 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.

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

l) 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.

6. **Termination.** This Appendix 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 Transfer covered by the Standard Contractual Clauses (and if such mechanism applies only to some of the data transfers, this Appendix will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Appendix.