SYNDIGO LLC
DATA PROCESSING ADDENDUM

Last updated: September 12, 2022

Clients

This Syndigo Data Processing Addendum (this "**Addendum**"), including its Exhibits (as defined in Section 12), is entered into by and between Syndigo LLC, a Limited Liability Company incorporated under the laws of the State of Delaware, and its relevant Affiliates (collectively, "**Syndigo**") and the entity signing the Syndigo Data Processing Addendum Accession Agreement (the "**Client**") (each, a "**Party**" and, collectively, the "**Parties**") as of the later of the signature dates included in the Syndigo Data Processing Addendum Accession Agreement, or the later of the signature dates included in an agreement that incorporates by reference this Addendum (the "**Effective Date**").

This Addendum forms part of the Syndigo Master Client Agreement or other mutually executed agreements (the "**Agreement**") between Syndigo and the Client applicable to Syndigo's provision of Services (as defined below) to the Client. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended or supplemented by, and including, this Addendum.

RECITALS

WHEREAS, the Parties entered into the Agreement and have retained the power to alter, amend, revoke, or terminate the Agreement as provided in the Agreement;

WHEREAS, the Parties now wish to amend the Agreement to ensure that Personal Data (as defined below) transferred between the Parties is Processed in compliance with applicable data protection principles and legal requirements.

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

1. Definitions

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

1.2. For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

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

(b) "**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including laws of the European Union (or any member state thereof) and the laws of any other country, province, or state to which the Processing of the Personal Data is subject, including the laws specified in **Exhibit B** hereto.

(c) "**Client**" means the party that has entered into this Addendum with Syndigo as indicated in the opening paragraph of this Addendum.

(d) "**Client Personal Data**" means any Personal Data Processed by Syndigo or a Contracted Processor on behalf of the Client (where the client is the Controller) pursuant to or in connection with the Agreement. For the avoidance of doubt, Personal Data processed by Syndigo or a Contracted Processor to respond to customer support queries is not considered Client Personal Data;

(e) "**Contracted Processor**" means any third party appointed by or on behalf of Syndigo to Process Personal Data on behalf of the Client in connection with the Agreement.

(f) "**GDPR**" or "**General Data Protection Regulation**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 "on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC," as may be amended from time to time.

(g) "**Personal Data Recipient**" means Syndigo, a Contracted Processor, or both collectively.

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

(i) "**Services**" means the services and other activities carried out by or on behalf of Syndigo for the Client pursuant to the Agreement.

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

1.3. The terms "**Controller**", "**Data Subject**", "**Data Processor**" or **"Joint Controller**", "**Processor**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Sub-Processor**" shall have the same meaning as in the GDPR (although shall apply per the terms of Section 2.1), and their cognate terms shall be construed accordingly.

2. Applicability

2.1. This Addendum will apply to the Processing of all Personal Data, regardless of country of origin, place of Processing, location of Data Subjects, or any other factor.

3. Processing and Disclosure of Client Personal Data

3.1. In the context of this Addendum and its exhibits, with regard to the Processing of Client Personal Data, the Client acts as a Controller and Syndigo acts as a Processor.

3.2. Syndigo shall:

(a) comply with all Applicable Data Protection Laws in the Processing of Client Personal Data;

(b) Process Client Personal Data solely on the Client's relevant documented instructions (including with regard to international transfers of Client Personal Data), unless such Processing is required by Applicable Data Protection Laws to which the relevant Personal Data Recipient is subject, in which case Syndigo shall, to the extent permitted by Applicable Data Protection Laws, inform the Client of that legal requirement before the respective act of Processing of that Client Personal Data;

(c) only conduct transfers of Client Personal Data in compliance with all applicable conditions, as laid down in Applicable Data Protection Laws;

(d) not retain, delete, or otherwise Process Client Personal Data contrary to or in the absence of the direct instructions of the Client, provided, however, that the Client expressly and irrevocably authorizes such retention, deletion, or other Processing if and to the extent required or allowed by Applicable Data Protection Laws; and

(e) immediately inform the Client in the event that, in Syndigo's opinion, a Processing instruction given by the Client may infringe Applicable Data Protection Laws.

3.3. The Client instructs Syndigo (and authorizes Syndigo to instruct each Contracted Processor) to Process Client Personal Data, and, in particular, transfer Client Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Agreement and this Addendum, and in particular to Contracted Processors. The Client acknowledges that the transfers of Client Personal Data to Contracted Processors are essential for the provision of the Services and accepts all liability for those transfers.

3.4. The Client represents and warrants that it has all necessary rights to provide the Client Personal Data to Syndigo for the purpose of Processing such data within the scope of this Addendum and the Agreement. Within the scope of the Agreement and in its use of the Services, the Client shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Client Personal Data to Syndigo and the Processing of Client Personal Data.

4. Syndigo Personnel

4.1. Syndigo shall take reasonable steps to ensure the reliability of any of its employees, agents, or contractors who may have access to Client Personal Data.

4.2. Syndigo shall ensure that access to Client Personal Data is strictly limited to those individuals who need to know or access it, as strictly necessary to fulfill the documented Processing instructions given to Syndigo by the Client or to comply with Applicable Data Protection Laws.

4.3. Syndigo shall ensure that all such individuals are subject to formal confidentiality undertakings, professional obligations of confidentiality, or statutory obligations of confidentiality.

5. Security of Processing

5.1. Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons, Syndigo shall, with regard to Client Personal Data, implement and maintain appropriate technical, administrative, and organizational security measures to ensure a level of security appropriate to that risk, as well as assist the Client with regard to ensuring compliance with the Client's obligations pursuant to the Applicable Data Protection Laws.

5.2. In assessing the appropriate level of security, Syndigo shall take account, in particular, of the risks that are presented by the nature of such Processing activities, and particularly those related to possible Personal Data Breaches.

5.3. The Client is responsible for reviewing information made available by Syndigo relating to data security and making an independent determination as to whether the listed security measures pertaining to the Services meet the Client's requirements and legal obligations under Applicable Data Protection Laws. The Client acknowledges that the security measures are subject to technical progress and development and that Syndigo may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Client.

5.4. Notwithstanding the above, the Client agrees that, except as provided by this Addendum, the Client is responsible for its secure use of the Services, including, but not limited to, securing its account authentication credentials and protecting the security of the Client Personal Data when in transit to and from the Services.

6. Sub-processing

6.1. The Client authorizes Syndigo to appoint (and permit each Contracted Processor appointed in accordance with this Section 6 to appoint) Contracted Processors in accordance with this Section 6 and any possible further restrictions, as set out in the Agreement.

6.2. Syndigo may continue to use those Contracted Processors already engaged by Syndigo as of the date of this Addendum, subject to Syndigo meeting the obligations set out in Section 6.4. The list of Syndigo's Contracted Processors as of the Effective Date is available at https://www.syndigo.com/subscription/clients/subprocessors/.

6.3. Syndigo shall provide the Client prior written notice of the appointment of any new Contracted Processor by updating the list of Syndigo Contracted Processors. If the Client requires prior notification of any updates to the list of Contracted Processors, the Client can subscribe to receive updates. If, within thirty (30) days of posting of each such notice, the Client notifies Syndigo in writing of any reasonable objections to the proposed appointment, Syndigo shall not appoint or disclose any Client Personal Data to that proposed Contracted Processor until reasonable steps have been taken to address the objections raised by the Client and, in turn, the Client has been provided with a reasonable written explanation of the steps taken to account for any such objections. If the Client, nevertheless, objects to the proposed appointment, it shall be entitled to terminate the Agreement as a remedy.

6.4. With respect to each Contracted Processor, Syndigo shall:

(a) carry out adequate due diligence to ensure that the Contracted Processor is capable of providing the level of protection and security for Client Personal Data required by this Addendum, the Agreement, and Applicable Data Protection Laws before the Contracted Processor first Processes Personal Data or, where applicable, in accordance with Section 6.2; and

(b) where required under the terms of **Exhibit B**, ensure that the arrangement between Syndigo and any prospective Contracted Processor is governed by a written contract that includes terms which offer at least the same level of protection for Client Personal Data as those set out in this Addendum (excluding its Exhibits).

7. Rights of the Data Subjects

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

7.2. With regard to the rights of the Data Subjects within the scope of this Section 7, Syndigo shall:

(a) promptly notify the Client if any Personal Data Recipient receives a request from a Data Subject under any Applicable Law with respect to Client Personal Data; and

(b) ensure that the Personal Data Recipient does not respond to that request, except on the documented instructions of the Client, or as required by Applicable Data Protection Laws to which the Personal Data Recipient is subject, in which case Syndigo shall, to the extent

permitted by Applicable Data Protection Laws, inform the Client of that legal requirement before the Personal Data Recipient responds to the request.

(c) Client shall provide Syndigo with instructions to respond to the request within five (5) days from the day Syndigo notified the Client of the request. If the Client does not provide such instructions within five (5) business days, Syndigo shall be authorized to provide the Client's contact details to the Data Subject in order to allow the Data Subject to submit their request directly to the Client.

8. Personal Data Breach

8.1. Syndigo shall notify the Client without undue delay upon Syndigo becoming aware of a Personal Data Breach affecting Client Personal Data under Syndigo's direct control or upon Syndigo being notified of a Personal Data Breach affecting Personal Data under the direct control of a Contracted Processor. The notification to the Client will include sufficient information to allow the Client to meet any applicable obligations pursuant to the Applicable Data Protection Laws (such as to report to the supervisory authorities or any other competent authorities or inform the Data Subjects of the Personal Data Breach).

8.2. Syndigo shall cooperate with the Client and take all reasonable commercial steps to assist the Client in the investigation, mitigation, and remediation of each such Personal Data Breach.

8.3. Syndigo's notification of or response to a Personal Data Breach under this Section 8 will not be construed as an acknowledgement by Syndigo of any fault or liability with respect to the Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

9.1. Syndigo shall provide the Client with relevant information and documentation with regard to any data protection impact assessments, and prior consultations with supervisory authorities, when the Client reasonably considers that such data protection impact assessments or prior consultations are required pursuant to Applicable Data Protection Laws, but in each such case solely with regard to Processing of Client Personal Data by, and taking into account the nature of the Processing and information available to Syndigo.

10. Deletion or Return of Client Personal Data

10.1. Upon termination or expiration of the Agreement, Syndigo shall, upon the Client's written request received by Syndigo within twenty-one (21) days of termination of the Service, at the choice of the Client, return or delete Client Personal Data and copies of such data in its custody and control, unless and only to the extent Applicable Data Protection Laws prevents it from returning or destroying all or part of Client Personal Data. For clarification, depending on the service plan purchased by the Client, access to export functionality may incur additional charge(s) and require purchase of an upgrade of the Services.

10.2. If Syndigo does not receive the Client's written request within twenty-one (21) days of termination of the Services, Syndigo shall delete Client Personal Data in accordance with Syndigo's data deletion policies and procedures. The Client expressly consents to such deletion.

11. Audit Rights

11.1. Where the Client is entitled to and desires to review Syndigo's compliance with this Addendum and the Applicable Data Protection Laws, the Client may request, and Syndigo will provide (subject to obligations of confidentiality), a copy of Syndigo's most recent System and Organization Controls (SOC) 2 Report or ISO 27001 certificate relevant to the Services, or any other relevant audit report Syndigo might have been issued.

11.2. If the Client, after having reviewed such audit report(s) and/or certificate(s), still reasonably deems that it requires additional information, Syndigo shall allow for and contribute to audits by the Client or an auditor mandated by the Client with regard to the Processing of the Client Personal Data by Syndigo, provided such audit will be conducted (1) during regular business hours; (2) without interfering with Syndigo's business operations or causing Syndigo to breach any legal or contractual obligation to which it is subject; (3) upon prior written notice received in a timely fashion and further consultation with Syndigo; (4) all subject to obligations of confidentiality; (5) at most, once a year; and (6) restricted to Client Personal Data. For the avoidance of doubt, audit means the provision of relevant documentation, email exchanges and interviews with members of the Syndigo Privacy Team.

11.3. The Client will bear its own expenses and agrees to pay Syndigo, upon receipt of invoice, a reasonable fee based on the time spent, as well as to account for the materials expended, in relation to the Client exercising its rights under this Section 11 or the Standard Contractual Clauses.

12. Exhibits to the Addendum

12.1. The Addendum includes the following exhibits (each, an "**Exhibit"**, and together, "**Exhibits**"):

(a) **Exhibit A** (Details of Processing)

(b) **Exhibit B** (Jurisdiction Specific Terms)

(c) **Exhibit C** (Supplementary Terms to the Standard Contractual Clauses)

12.2. From time to time, Syndigo may unilaterally update the terms included in the Exhibits listed in Section 12.1 by posting updated terms to the page(s) where such Exhibits are posted. If the Client does not object to the updated Exhibit within fourteen (14) days from the date the update was posted, the Client will be deemed to have consented to the updated Exhibit. Syndigo shall only update the Exhibits as follows:

(a) Syndigo may only unilaterally update the terms of **Exhibit A** to reflect changes to the details of Processing of Client Personal Data that may arise from changes to the Services or to provide additional information required to conclude the Standard Contractual Clauses.

(b) Syndigo may only unilaterally update the terms of **Exhibit B** to reflect changes in or additions to Applicable Data Protection Laws to which the Processing is subject (or may be subject to).

(c) Syndigo may only unilaterally update the terms of **Exhibit C** to reflect changes to the supplementary measures required to conduct Restricted Transfers under the Standard Contractual Clauses (as defined by the applicable sections of **Exhibit B**).

12.3. In case of any conflict or ambiguity between the terms of **Exhibit B** and any other terms of the body of this Addendum, the applicable terms of **Exhibit B** will take precedence.

12.4. Syndigo shall provide Client notification of changes to the Exhibits by offering Client a mechanism to subscribe to updates to the Exhibits.

13. Restricted Transfers

13.1. Restricted Transfers of Client Personal Data within the scope of this Addendum shall be conducted in accordance with the applicable terms and requirements of **Exhibit B**.

13.2. Where the Standard Contractual Clauses (as specified under **Exhibit B**) are the applicable data transfer mechanism according to the terms and requirements set out in **Exhibit B**, the applicable Standard Contractual Clauses will be the clauses applicable to the role of the Parties as described in Section 3.1.

14. No Selling of Client Personal Data

14.1. Syndigo acknowledges and confirms that it does not receive any Client Personal Data as consideration for any Services or other items that Syndigo provides to the Client. The Client retains all rights and interests in its Client Personal Data. The Client agrees to refrain from taking any action that would cause any transfers of Client Personal Data to or from Syndigo to qualify as selling Client Personal Data under Applicable Data Protection Laws.

15. Indemnification

15.1. The Client agrees to indemnify and hold harmless Syndigo and its officers, directors, employees, agents, affiliates, successors, and permitted assigns against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind which Syndigo may sustain as a consequence of the breach by the Client of its obligations pursuant to the Applicable Data Protection Laws or this Addendum.

16. General Terms

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

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

16.3. In the event of any conflict between the Agreement (including any annexes and appendices thereto) and this Addendum, the provisions of this Addendum shall control.

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

16.5. If Syndigo determines that it can no longer meet any of its obligations in accordance with this Addendum, it shall promptly notify the Client of that determination, and cease the Processing or take other reasonable and appropriate steps to remediate.

16.6. If you are accepting the terms of this Addendum on behalf of an entity, you represent and warrant to Syndigo that you have the authority to bind that entity and its affiliates, where applicable, to the terms and conditions of this Addendum.

17. Data Protection Officer

17.1. The Data Protection Officer of Syndigo is:

VeraSafe, LLC
100 Street S.E., Suite 600
Washington, D.C. 20003

USA
Phone: +1 (617) 398-7067
Email: experts@verasafe.com
Web: https://www.verasafe.com/about-verasafe/contact-us/

18. Data Protection Representatives

18.1. The European Union Representative of Syndigo pursuant to Article 27 of the GDPR is:

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

VeraSafe Ireland Ltd
Unit 3D North Point House,
North Point Business Park,
New Mallow Road, Cork T23AT2P
Ireland

Contact form: https://www.verasafe.com/privacy-services/contact-article-27-representative/

18.2. The United Kingdom ("**UK**") Representative of Syndigo pursuant to Article 27 of the UK GDPR (as defined in the Jurisdiction Specific Terms located in **Exhibit B**) is:

VeraSafe United Kingdom Ltd.
37 Albert Embankment
London SE1 7TL
United Kingdom Email: experts@verasafe.com
Web: https://www.verasafe.com/about-verasafe/contact-us/

19. Notices under the Addendum

19.1. Notices to Syndigo under the Addendum shall be directed to privacy@syndigo.com.

19.2. Client shall provide the contact details for the purpose of receiving notices under the Addendum to privacy@syndigo.com.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

Exhibit A

Details of Processing

1. Further details of the Processing, in addition to the ones laid down in the Agreement and this Addendum, include:

1.1. The subject matter of the Processing of Client Personal Data is:

(a) The subject matter of the Processing of Client Personal Data pertains to the provision of Services (content and brand management services), as requested by the Client.

1.2. The duration of the Processing of Client Personal Data is:

(a) The duration of the Processing of Client Personal Data is generally determined by the Client and is further subject to the terms of this Addendum and the Agreement, respectively, in the context of the contractual relationship between Syndigo and the Client.

1.3. The nature and purpose of the Processing of Client Personal Data is:

(a) The purpose of Processing of Personal Data is to:

(i) provide the Data Subjects with access to the Services

(ii) enable the Data Subject's use of the Services

(iii) notify the Data Subjects about changes to the Services

1.4. The categories of Client Personal Data to be Processed are:

(a) Biographical information (such as first and last name)

(b) Professional information (such as role/job title and company name)

(c) Contact information (such as email address, physical address, phone number, and username)

(d) Web analytics data (such as data obtained with session and persistent cookies)

(e) Information voluntarily provided by the Data Subjects in free-text boxes

1.5. The Special Categories of Client Personal Data to be Processed, and the applied restrictions to the Processing of such Special categories of Personal Data are:

(a) No special categories of Client Personal Data are to be Processed.

1.6. The categories of Data Subjects to whom the Client Personal Data relates are:

(a) The Client's employees or contractors authorized by the Client to use the Services

(b) Any additional users of the Services authorized by the Client to use the Services

(c) The Client's business partners or contacts authorized by the Client to use the Services

1.7. Description of the technical, administrative, and organizational security measures implemented by Syndigo can be found at https://syndigo.com/security-and-reliability/.

1.8. With respect to Processing activities carried out by Contracted Processors: Syndigo has a vendor management procedure that includes an exhaustive review of data processing agreements against the requirements of Data Protection Laws and a security audit which includes review of relevant information security certifications such as SOC 2 audit reports, ISO 27001 certifications, completion of security questionnaires and review of supporting documentation.

1.9. The basic Processing activities to which the Client Personal Data will be subject include, without limitation:

(a) Collection, organization, storage, adaptation or alteration as requested by the Client or the Data Subjects, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, erasure, or destruction for the purpose of providing the Services to the Client in accordance with the terms of the Agreement.

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

(a) The frequency of the transfer of Client Personal Data is determined by the Client. Client Personal Data may be transferred each time that Client instructs Syndigo to process Personal Data.

1.11. Maximum data retention periods, if applicable:

(a) The retention period of Client Personal Data is generally determined by the Client and is subject to the term of this Addendum and the Agreement, respectively, in the context of the contractual relationship between Syndigo and the Client.

1.12. Further Processing:

(a) Syndigo and its Contracted Processors shall not carry out further Processing on Client Personal Data.

1.13. The following is deemed an instruction by the Client to Process Client Personal Data in the following manners:

(a) Processing in accordance with the Agreement;

(b) Processing initiated by Data Subjects in their use of the Services; and

(c) Processing to comply with other reasonable documented instructions provided by the Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.

Exhibit B

Jurisdiction Specific Terms

1. European Economic Area

1.1. Definitions.

(a) "**EU 2021 Standard Contractual Clauses**" 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.

(b) "**European Economic Area**" ("**EEA**") means the EU Member States, and Iceland, Liechtenstein, and Norway.

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

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

(e) "**Third Country**" means a country outside of the EEA.

1.2. Agreements with Contracted Processors

(a) Syndigo shall ensure that the arrangement between Syndigo and any prospective Contracted Processor is governed by a written contract that includes data protection obligations that offer at least the same level of protection for Personal Data as those set out under the Addendum (excluding its Exhibits) and this Section 1. Client agrees that older versions of the Standard Contractual Clauses concluded between Syndigo and Contracted Processor offer at least the same level of protection for Personal Data as those set out under the Addendum (excluding its Exhibits) and this Section 1.

1.3. Restricted Transfers of EEA Personal Data

(a) With regard to any Restricted Transfer of EEA Personal Data from the Client to Syndigo within the scope of this 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 that provides that the Third Country, a territory, or one or more specified sectors within that Third Country, or the international organization in question to which Personal Data is to be transferred ensures an adequate level of data protection.

(ii) Syndigo's certification to any successor to the EU-U.S. Privacy Shield Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the GDPR), provided that the Services are covered by the certification.

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

(iv) Any other lawful data transfer mechanism, as laid down in the GDPR, as the case may be.

(b) This Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses (which may be updated from time to time if required by law or at the choice of Syndigo to reflect the latest version adopted by the European Commission), provided that the content of the annexes of the EU 2021 Standard Contractual Clauses is set forth in **Exhibit A** to this Addendum. The Parties are deemed to have accepted, executed, and signed the EU 2021 Standard Contractual Clauses where necessary in their entirety (including the annexes thereto). For the purpose of the EU 2021 Standard Contractual Clauses and this Section 1:

(i) Syndigo shall be deemed the "data importer" and the Client the "data exporter." The text contained in **Exhibit C** to this Addendum serves to supplement the Standard Contractual Clauses.

(ii) The Parties agree to the terms in module two of the EU 2021 Standard Contractual Clauses when, in accordance with Section 3.1 of the Addendum, the Data Exporter is Client and acts as a Controller and the Data Importer is Syndigo and acts as a Processor.

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

(iv) With respect to Clause 9, the Parties select the "Option 2 General Written Authorisation" under Modules Two and Three, and the time period set forth in Section 6.4 of the Addendum.

(v) With respect to Clause 11, the Parties agree not to provide the right to lodge a complaint with an independent dispute resolution body.

(vi) With respect to Clause 13 and Annex I.C, the competent supervisory authority shall be determined by the location of the data exporter or its data protection representative in the EEA. If the data exporter is not established in an EEA country and the processing activities are subject to the GDPR by virtue of application of Article 3(2) GDPR, and the data exporter does not have a data protection representative under Article 27 GDPR, the exporter chooses the Data Protection Commission (Ireland).

(vii) With respect to Clause 17 of the EU 2021 Standard Contractual Clauses, the Parties select, under Option 1, the law of the Republic of Ireland.

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

(ix) The additional safeguards identified in **Exhibit C** supplement the EU 2021 Standard Contractual Clauses.

(x) 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 Standard Contractual Clauses shall prevail.

2. California

2.1. Definitions.

(a) "**Applicable Data Protection Laws**" (as used in the Addendum) includes the California Consumer Privacy Act of 2018, Assembly Bill 375 of the California House of Representatives, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy and approved by the California Governor on June 28, 2018 ("**CCPA**") and the California Consumer Privacy Act Regulations ("**CCPA Regulations**"), in addition to the California Privacy Rights Act of 2020 ("**CPRA**") where in force, as may be amended from time to time.

(b) "**Business Purpose**" (as used in this Section) shall have the same meaning as in the CCPA.

(c) "**Commercial Purpose**" (as used in this Section) shall have the same meaning as in the CCPA.

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

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

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

(g) "**Personal Data Breach**" (as used in the Addendum) includes "**Breach of the Security of the System**" as defined under the CCPA.

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

2.2. The Client discloses Client Personal Data to Syndigo solely for: (i) valid Business Purposes as permitted by the Applicable Data Protection Laws; and (ii) to enable Syndigo to perform the Services under the Agreement.

2.3. Syndigo shall not: (i) sell or share Client Personal Data, as the terms are understood under Applicable Data Protection Laws; (ii) retain, use, or disclose Client Personal Data for a Commercial Purpose other than providing the Services specified in the Agreement or as otherwise permitted by Applicable Data Protection Laws; nor (iii) retain, use, or disclose Personal Data except where permitted under the Agreement between the Client and Syndigo or as otherwise permitted by the Applicable Data Protection Laws. Syndigo certifies that it understands these restrictions and will comply with them.

2.4. Agreements with Contracted Processors.

(a) Syndigo shall ensure that the arrangement between Syndigo and any prospective Contracted Processor is governed by a written contract that includes data protection obligations that offer at least the same level of protection for Client Personal Data as those set under this Section 2. Client agrees that agreements between Contracted Processors and Syndigo that do not specifically include Client Personal Data governed by the CCPA provide data protection obligations compatible with those of Syndigo under the Addendum and this Section 2.

3. Canada

3.1. Definitions.

(a) "**Applicable Data Protection Laws**" (as used in the Addendum) includes the Canadian Federal Personal Information Protection and Electronic Documents Act ("**PIPEDA**").

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

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

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

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

3.3. Agreements with Contracted Processors.

(a) Syndigo shall ensure that the arrangement between Syndigo and any prospective Contracted Processor is governed by a written contract that includes data protection obligations that offer at least the same level of protection for Client Personal Data as those set out under the Addendum (excluding its Exhibits) and this Section 3. Client agrees that agreements between Syndigo and Contracted Processors that do not specifically include Client Personal Data governed by PIPEDA provide data protection obligations compatible with those of Syndigo under the Addendum and this Section 3.

4. Switzerland

4.1. "**Applicable Data Protection Laws**" (as used in the Addendum) includes the Federal Act on Data Protection of 19 June 1992 ("**FADP**") and the Ordinance to the Federal Act on Data Protection ("**OFADP**"), as may be amended from time to time.

4.2. "**EU 2021 Standard Contractual Clauses**" 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.

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

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

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

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

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

4.8. "**Supervisory Authority**" (as used in the Addendum) includes the Federal Data Protection and Information Commissioner.

4.9. "**Third Country**" means a country outside of the Swiss Confederation.

4.10. With regard to any Restricted Transfer of Swiss Personal Data from the Client to Syndigo within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

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

(b) Syndigo's certification to any successor to the Swiss-U.S. Privacy Shield Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the FADP and the OFADP, as the case may be), provided that the Services are covered by the self-certification.

(c) The EU 2021 Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under Article 6.2 (a) of the FADP).

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

4.11. EU 2021 Standard Contractual Clauses:

(a) This Addendum incorporates by reference the EU 2021 Standard Contractual Clauses provided that the content of Annex I.B and Annex II is set forth in **Exhibit A** to the Addendum.

(b) This Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses (which may be updated from time to time if required by law or at the choice of Syndigo to reflect the latest version adopted by the European Commission), provided that the content of the annexes of the EU 2021 Standard Contractual Clauses is set forth in **Exhibit A** to this Addendum. The Parties are deemed to have accepted, executed, and signed the EU 2021 Standard Contractual Clauses where necessary in their entirety (including the annexes thereto). For the purpose of the EU 2021 Standard Contractual Clauses and this Section 1:

(i) Syndigo shall be deemed the "data importer" and the Client the "data exporter." The text contained in **Exhibit C** to this Addendum serves to supplement the Standard Contractual Clauses.

(ii) The Parties agree to apply module two of the EU 2021 Standard Contractual Clauses when, in accordance with Section 3.1 of the Addendum, the Data Exporter is Client and acts as a Controller and the Data Importer is Syndigo and acts as a Processor.

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

(iv) With respect to Clause 9, the Parties select the "Option 2 General Written Authorisation" under Modules Two and Three, and the time period set forth in Section 6.4 of the Addendum.

(v) With respect to Clause 11, the Parties agree not to provide the right to lodge a complaint with an independent dispute resolution body.

(vi) With respect to Clause 13 and Annex I.C, the competent authority shall be the Swiss Federal Data Protection and Information Commissioner, insofar as the data transfer constitutes a Restricted International Transfer of Swiss Personal Data.

(vii) With respect to Clause 17, the Parties select, under Option 1, the law of law of the Swiss Confederation.

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

(ix) The additional safeguards identified in **Exhibit C** supplement the EU 2021 Standard Contractual Clauses.

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

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

(c) 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 EU 2021 Standard Contractual Clauses shall prevail.

5. United Kingdom

5.1. Definitions.

(a) "**Applicable Data Protection Laws**" (as used in the Addendum) includes the Data Protection Act 2018 and the UK GDPR (as defined below).

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

(c) "**UK GDPR**" (as used in this Section) means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 "on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)" as has been amended, adopted, and forming part of the law of England, Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdraw) Act 2020.

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

(e) "**UK International Data Transfer Addendum**" means the International Data Transfer Addendum to the EU 2021 Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 and available at

https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf).

5.2. UK Restricted Transfers:

(a) With regard to any UK Restricted Transfer from the Client to Syndigo within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(i) A valid adequacy decision pursuant to the requirements under the UK GDPR and the Data Protection Act 2018 that provides that the Third Country, a territory, or one or more specified sectors within that Third Country, or the international organization in question to which Personal Data is to be transferred, ensures an adequate level of data protection.

(ii) Syndigo's certification to any successor to the EU-U.S. Privacy Shield Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the UK GDPR and the Data Protection Act 2018, as the case may be), provided that the Services are covered by the self-certification.

(iii) The UK International Data Transfer Addendum (in so far as its use constitutes an "appropriate safeguard" under the UK GDPR and the Data Protection Act 2018.)

(b) For data transfers from the UK that are subject to the UK International Data Transfer Addendum, the UK International Data Transfer Addendum will be deemed entered into (and incorporated into this Addendum by reference) and completed by the Parties as follows:

(i) For the purposes of Table 1 of the UK International Data Transfer Addendum, the Parties' details and key contact information are located in Section 17 and Section 18 of this Addendum.

(ii) For the purposes of Table 2 of the UK International Data Transfer Addendum, information about the version of the Approved EU 2021 Standard Contractual Clauses, modules and selected clauses which the UK International Data Transfer Addendum is appended to is located in Section 1.3(b) of this **Exhibit B**.

(iii) For the purposes of Table 3 of the UK International Data Transfer Addendum:

- The Parties' details are found in the Agreement.
- The description of the transfer is set forth in **Exhibit A**.
- The contents of Annex II are included in Section 1.7 of **Exhibit A** and in **Exhibit C**.
- The list of sub-processors is located at https://www.syndigo.com/subscription/clients/subprocessors/.

(iv) For the purposes of Table 4 of the UK International Data Transfer Addendum, both the Data Importer and the Data Exporter may end the UK International Data Transfer Addendum in accordance with the terms of the UK International Data Transfer Addendum.

(c) To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Addendum and any other terms in this

Addendum, the provisions of the EU 2021 Standard Contractual Clauses or UK International Data Transfer Addendum, as applicable, will prevail.

5.3. Agreements with Contracted Processors:

(a) Syndigo shall ensure that the arrangement between Syndigo and any prospective Contracted Processor is governed by a written contract that includes data protection obligations that offer at least the same level of protection for Client Personal Data as those set out in this Addendum and this Section 5. Client agrees that agreements between Contracted Processors and Syndigo that do not specifically include Client Personal Data protected by the UK GDPR provide data protection obligations compatible with those of Syndigo under the Addendum and this Section 5. Client agrees that older versions of the Standard Contractual Clauses concluded between Syndigo and Contracted Processor offer at least the same level of protection for Personal Data as those set out under the Addendum (excluding its Exhibits) and this Section 5.

6. Brazil

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

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

6.3. "**LGPD**" means Lei Geral de Proteção de Dados, Law No. 13.709 of 14 August 2018, Brazil's General Data Protection Law.

6.4. "**Personal Data Breach**" (as used in the Addendum) includes "**Incidente de segurança**" as used under the LGPD.

6.5. "**Processor**" includes "**Operador**" as defined under the LGPD.

Exhibit C

Supplementary Terms to the Standard Contractual Clauses

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

1. Applicability of this Exhibit

1.1. This Exhibit only applies with respect to Restricted Transfers of Client Personal Data when the Parties have concluded the Standard Contractual Clauses pursuant to the Addendum and its Exhibits and the applicable terms in **Exhibit C** indicate that **Exhibit C** applies to the Restricted Transfer.

2. Definitions

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

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

(b) "**Data Importer**" and "**Data Exporter**" shall have the same meaning provided under the Standard Contractual Clauses.

(c) "**Disclosure Request**" means any request from law enforcement authority or other governmental authority with competent authority and jurisdiction for disclosure of Personal Data.

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

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

3. Applicability of Surveillance Laws to Data Importer

3.1. U.S. surveillance laws:

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

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

(i) No court has found Data Importer to be an entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication Data Importer" within the

meaning of 50 U.S.C. § 1881(b)(4); or (ii) a member of any of the categories of entities described within that definition.

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

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

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

(a) Data Importer commits to provide, upon request, information about the laws and regulations in the destination countries of the transferred data applicable to Data Importer that would permit access by public authorities to the transferred Client Personal Data, in particular in the areas of intelligence, law enforcement, or administrative and regulatory supervision applicable to the transferred Client Personal Data. In the absence of laws governing the public authorities' access to Personal Data, Data Importer shall provide Data Exporter with reasonable information and statistics based on the experience of Data Importer or reports from various sources on access and Disclosure Requests by public authorities to Personal Data in situations similar to the Restricted Data Transfer. Data Importer may choose the means to provide the information.

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

4. Obligations on Data Importer in the Event of Receiving a Disclosure Request

1.1. In the event Data Importer receives a Disclosure Request subject to the Addendum that has been transferred under the Standard Contractual Clauses, Data Importer shall comply with the following, unless prohibited under the law applicable to Data Importer:

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

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

(c) Use all lawful efforts to challenge the Disclosure Request the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable EEA Member State law or any other Applicable Data Protection Law and demand that the public authority aims to obtain such information via

co-operation with government bodies in each jurisdiction (such as using an alternative established treaty or mechanism to allow government-government sharing of information). For the purpose of this Exhibit, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

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

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

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

(g) Document all the steps taken by Data Importer related to the Disclosure Request.

5. Information on Disclosure Requests for Personal Data by Public Authorities

5.1. Where allowed by law and upon the Data Exporter's request, Data Importer commits to provide Data Exporter with sufficiently detailed information on all requests of access to Personal Data by public authorities which Data Importer has received over the last ten (10) years in particular in the areas of intelligence, law enforcement, administrative, and regulatory supervision applicable to the transferred data and comprising information about the requests received, the data requested, the requesting body, and the legal basis for disclosure and to what extent Data Importer has disclosed the requested data. Data Importer may choose the means to provide this information.

6. Backdoors

6.1. Data Importer certifies that:

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

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

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

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

7. Information About Legal Prohibitions

7.1. Data Importer will provide Data Exporter information about the legal prohibitions on Data Importer to provide information under Sections 5 through 6 of this Exhibit. Data Importer may choose the means to provide this information.

8. Other Measures to Prevent Authorities from Accessing Client Personal Data

1.2. Notwithstanding the application of the security measures set forth in the Addendum, Data Importer will implement, where feasible, the following technical, organizational, administrative, and physical measures designed to protect the transferred Client Personal Data from unauthorized disclosure or access:

(a) Encryption of the transferred Client 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 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 unauthorized software applications and IT systems for vulnerabilities of Data Importer;

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

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

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

(h) Internal policies establishing that:

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

ii. Data Importer must require an official, signed document issued pursuant to the applicable laws of the requesting public authority before it will consider a Disclosure Request for transferred Client Personal Data;

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

iv. If Data Importer is legally required to comply with a Disclosure Request, it will respond as narrowly as possible to the specific Disclosure Request.

9. Inability to Comply with this Exhibit

9.1. Data Importer shall promptly inform Data Exporter of its inability to comply with the Standard Contractual Clauses and this Exhibit.

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

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

9.4. Data Importer shall provide the Data Exporter with sufficient indications to exercise its duty to suspend or end the transfer and/or terminate the Agreement.

10. Conflicts with the Standard Contractual Clauses

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

11. Termination

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