SYNDIGO LLC DATA PROCESSING ADDENDUM

Last updated: August 1, 2024

Clients

This Syndigo Data Processing Addendum (this "**Addendum**"), including its Exhibits, 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 ("**Client**") which executed the Syndigo Master Client Agreement or other written or electronic agreement between Syndigo and Client ("**Agreement**") (each, a "**Party**" and, collectively, the "**Parties**").

By signing the Agreement, Client enters into this Addendum on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent Syndigo Processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this Addendum only, and except where indicated otherwise, the term "Client" shall include Client and Authorized Affiliates.

This DPA forms part of the Agreement as of the later of the signature dates included in the Agreement, or the Syndigo LLC Data Processing Addendum Accession Agreement (the "**Effective Date**").

RECITALS

WHEREAS, Syndigo provides the Services to the Client and in rendering the Services, Syndigo will Process the Client Personal Data on behalf of Client;

WHEREAS, the Parties agree to comply with the provisions in this Addendum as it relates to the Processing of Client Personal Data.

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 Client Personal Data under the Agreement, including the laws specified in **Exhibit B** hereto as may be amended, modified, or supplemented from time to time, as applicable.

(c) "**Authorized Affiliate**" means any Client Affiliate(s) which are subject to Applicable Data Protection Laws and are permitted to use the Services pursuant to the Agreement but have not signed their own order form or agreement with Syndigo.

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

(e) "**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, the Processing of Personal Data Processed by Syndigo as a controller is described in Syndigo's privacy notice, available on its website, and is not subject to the provisions of this Addendum.

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

(g) "**Data Exporter**" and "**Data Importer**" have the meanings assigned to them in **Exhibit A**.

(h) "**GDPR**" means the EU GDPR and UK GDPR as those terms are defined within **Exhibit B**, as applicable.

(i) "**Jurisdiction Specific Terms**" means all terms applicable to the Processing of Client Personal Data that apply to the extent that Syndigo Processes Client Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions identified in these terms. The Jurisdiction Specific Terms are currently available as **Exhibit B** to this Addendum.

(j) "**Restricted Transfer**" means any transfer of Client Personal Data subject to Applicable Data Protection Laws to Third Country or an international organization in a Third Country (including data storage on foreign servers).

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

(l) "**Standard Contractual Clauses**" are the model clauses for Restricted Transfers adopted by the relevant authorities of the jurisdictions indicated in **Exhibit B**, insofar as their use is approved by the relevant authorities as an appropriate mechanism or safeguard for Restricted Transfers.

(m) "**Sub-Processor**" means a direct Processor of a Processor. For the avoidance of doubt, Contracted Processors are Sub-Processors.

1.3. The terms "**Controller**", "**Data Subject**", "**Data Processor**" or **"Joint Controller**", "**Processor**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Sub-Processor**", "**Supervisory Authority**", and "**Third Country**" shall have the same meaning as in Applicable Data Protection Laws, and their cognate terms shall be construed accordingly.

2. Scope and Applicability

2.1. Scope. This Addendum will apply to the Processing of all Client Personal Data by Syndigo, regardless of country of origin, place of Processing, location of Data Subjects, or any other factor. For the avoidance of doubt, this Addendum does not apply to Client Personal Data that is aggregated, deidentified or anonymized nor shall restrict the ability of Syndigo to aggregate, deidentify or anonymize Client Personal Data.

2.2. Duration. This Addendum shall take effect on the Effective Date and shall continue concurrently for the duration that Client Personal Data is Processed by Syndigo pursuant to the Agreement.

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. The details of processing the Client Personal Data are set out in **Exhibit A**.

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 Restricted Transfers), 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 the 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. 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.

3.5. 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. Client shall have sole responsibility for the accuracy, quality, and legality of Client Personal Data and the means by which Client acquired such Client Personal Data. Client specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted out from sales or other disclosures of their Personal Data to the extent applicable under Applicable Data Protection Laws. 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. Authorization for Existing Contracted Processors. Client authorizes Syndigo to continue using those Contracted Processors already engaged by Syndigo as of the Effective Date, and further authorizes Syndigo and its Contracted Processors to appoint additional Contracted Processors provided obligations set out in Section 6.4 are met. The list of Syndigo's Contracted Processors as of the Effective Date is available at https://www.syndigo.com/subscription/clients/subprocessors/.

6.2. Authorization for Appointment of Contracted Processors. 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 at the following address: https://www.syndigo.com/subscription/clients/subprocessors/.

6.3. Objection to Contracted Processors.

(a) Client will be deemed to have consented to the additional Contracted Processor if no objection is received within fourteen (14) days of Syndigo's notice. Client may object to the appointment of a Contracted Processor by providing a written objection, which shall include the name of the objected-to Contracted Processor and a reasonable statement of objection.

(b) If an objection is received, the Parties will work together in good faith with a view of achieving a commercially reasonable resolution. If no mutually agreeable resolution is available, Client may terminate the Agreement immediately upon written notice to Syndigo, with no further fees due, other than what has been accrued up to and including the date of termination. Upon notice of termination, Syndigo shall cease Processing Client Personal Data.

6.4. Requirements for Appointing Contracted Processors. With respect to each Contracted Processor, Syndigo shall:

(a) conduct 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. Upon request, Syndigo will disclose the results of such due diligence to Client; and

(b) restrict the Contracted Processor's access to the Client Personal Data only to what is necessary to assist Syndigo in providing the Services, and prohibit the Contracted Processor from accessing Client Personal Data for any other purpose; and

(c) ensure that the arrangement between Syndigo and the 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.

6.5. Where any Contracted Processor fails to fulfil its data protection obligations under such written contract (or in the absence thereof, as the case may be), Syndigo shall remain fully liable to Client for the performance of the respective Contracted Processors' data protection obligations under such contract and/or Applicable Data Protection Laws.

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. Breach Response. If Syndigo discovers, is notified of, or has reason to suspect a Personal Data Breach affecting Client Personal Data under its or its Contracted Processors' control, Syndigo will (i) immediately implement measures to stop the unauthorized access; (ii) secure Client Personal Data; and (iii) shall notify the Client without undue delay upon Syndigo becoming aware of a Personal Data Breach affecting Client Personal Data.

8.2. Breach Obligations. Immediately upon providing notice of a Personal Data Breach, Syndigo shall:

(a) describe to Client in as much detail as reasonably possible: (i) the nature of the Personal Data Breach, (ii) where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, (iii) the impact of such Personal Data Breach upon Client and the affected Data Subjects, and (iv) the measures taken or proposed by Syndigo to address the Personal Data Breach;

(b) provide and supplement notifications as and when additional information becomes available;

(c) assist Client in meeting its respective obligations pursuant to Applicable Data Protection Laws, including any obligations to notify Supervisory Authorities or Data Subjects of a Personal Data Breach; and

(d) use commercially reasonable efforts to investigate, mitigate, and remediate each such Personal Data Breach and prevent a recurrence of such Personal Data Breach.

8.3. No Acknowledgement of Fault. 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 and its Contracted Processors.

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. To request a copy of these documents, email privacy@syndigo.com.

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. Jurisdiction Specific Terms.

To the extent Syndigo Processes Client Personal Data originating from or protected by Applicable Data Protection Laws in a jurisdiction listed in **Exhibit B**, then the terms and definitions specified in **Exhibit B** with respect to the applicable jurisdiction shall apply in addition to the terms of the body of this Addendum.

13. Restricted Transfers.

13.1. Restricted Transfers of Client Personal Data within the scope of this Addendum shall be conducted in accordance with **Exhibit B** and Applicable Data Protection Laws.

13.2. If the relevant authorities adopt a new version of Standard Contractual Clauses as a lawful mechanism for Restricted Transfers in a jurisdiction governing the processing of Client Personal Data, the Parties are deemed to have agreed to the execution of the new version of the Standard Contractual Clauses by signing this Addendum, and, if necessary, Syndigo shall be entitled to update **Exhibit A** and **Exhibit B** (and their appendices) accordingly.

13.3. If an alternative transfer mechanism, such as Binding Corporate Rules, is adopted by Syndigo during the term of the Agreement (an "**Alternative Mechanism**"), and Syndigo notifies Client that some or all Restricted Transfers can be conducted in compliance with Applicable Data Protection Laws pursuant to the Alternative Mechanism, the Parties will rely on the Alternative Mechanism instead of the transfer mechanisms in **Exhibit B** for Restricted Transfers to which the Alternative Mechanism applies.

13.4. In addition, Syndigo is certified to the EU-U.S. and Swiss-U.S. Data Privacy Frameworks, the UK Extension to the EU-U.S. Data Privacy Framework (together the "**Data Privacy Frameworks**") and the commitments they entail. Syndigo agrees to notify Client if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the principles of the Data Privacy Frameworks.

14. Exhibits to the Addendum

14.1. 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)

14.2. From time to time, Syndigo may unilaterally update the terms included in the Exhibits listed in Section 14.1 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**).

14.3. 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.

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

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.

15.2. The liability of each Party under this Addendum shall be subject to any exclusions and limitations of liability set out in the Agreement.

16. General Terms

16.1. Notice. Notices to Syndigo under the Addendum shall be directed to privacy@syndigo.com. Client shall provide the contact details for the purpose of receiving notices under the Addendum to privacy@syndigo.com.

16.2. Prior Existing Agreements: 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. 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. Conflict: 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. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this Addendum, the applicable Jurisdiction Specific Terms will prevail.

16.4. Severability: 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. Non-Compliance: If Syndigo determines that it can no longer meet any of its obligations in accordance with this Addendum, Applicable Data Protection Laws, or the Standard Contractual Clauses (as applicable), it shall promptly notify the Client of that determination, and cease the Processing or take other reasonable and appropriate steps to remediate.

16.6. Ambiguity. Syndigo may amend this Addendum without notice to or consent of Client for the purposes of a) curing any ambiguity, b) curing, correcting, or supplementing any defective provision contained herein, or c) making any other provisions with respect to matters or questions arising under this Addendum; provided that such action shall not materially alter the Addendum.

16.7. Signature: 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.

16.8. Disclosure to Supervisory Authorities. The Parties acknowledge that either Party may disclose this Addendum and any relevant privacy provisions in the Agreement to Supervisory Authorities, or any other judicial or regulatory body, upon their request.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

Exhibit A

Details of Processing

Name and Address of Parties:	**Syndigo:** Syndigo LLC and its relevant Affiliates **Client:** The Syndigo client identified, and which executed the Agreement.
Data Protection Contact:	**Syndigo**: Data Protection Officer: 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/ **Client:** Where relevant, Client shall notify Syndigo of its data protection contact or data protection officer via email: privacy@syndigo.com
Article 27 EU Representative:	**Syndigo**: VeraSafe Ireland Ltd, Unit 3D North Point House, North Point Business Park, New Mallow Road, Cork, T23AT2P, Ireland, Email: experts@verasafe.com, Web: https://www.verasafe.com/about-verasafe/contact-us/ **Client**: Where relevant, Client shall notify Syndigo of its Article 27 EU Representative via email: privacy@syndigo.com
Article 27 UK Representative:	**Syndigo:** 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/ **Client:**

	Where relevant, Client shall notify Syndigo of its Article 27 UK Representative via email: privacy@syndigo.com
Controllership Role:	As set forth in Section 3.1 of this Addendum.
Data Transfer Role:	Syndigo is the Data Importer; Client is the Data Exporter.
Subject Matter of the Processing Client Personal Data:	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.
Categories of Data Subjects to whom the Client Personal Data relates:	• The Client's employees, contractors, additional users, or business partners authorized by the Client to use the Services Applicable to Enhanced Content only: • Website visitors to Client's website where Enhanced Content is used
Categories of Client Personal Data Processed by Syndigo:	• The Client's employees, contractors, additional users, or business partners authorized by the Client to use the Services: ○ Biographical information: first name, and last name ○ Professional information: such as role/job title and company name (optional) ○ Contact information: business email address, physical address, phone number (optional) ○ Account information: username, application role (e.g., administrator or user), logs of data changes made by the user, password (hashed) Applicable to Enhanced Content only: • Website visitors to Client's website where Enhanced Content is used: ○ Web analytics including: ▪ User ID (GUID), session ID, visitor ID (random GUID), and IP address (the IP address is momentarily collected and then removed, it is never stored) ▪ User agent ▪ City code, continent code, country code, country name, region, state ▪ Browser information such as pageviews and time on page ▪ Transactional event which are native to Enhanced Content's delivery process such as content loaded, content displayed, interactions with content, and conversations

	All of this raw data is aggregated by Syndigo and not accessible in its raw form to the Client. No special categories of Client Personal Data are to be Processed.
Purpose of Processing Client Personal Data:	The Processing is related to the provision of Services to Client as further detailed within the Agreement and the provision of aggregate information pertaining to interactions with Enhanced Content to suppliers, including but not limited to collection, storage, analysis, masking, aggregation and deletion. Syndigo and its Contracted Processors (if applicable) will perform such acts of Processing of Client Personal Data as are necessary to provide those Services according to Client's instructions. The purpose of Processing Client Personal Data is: • To provide the Data Subjects with access to the Services • To enable the Data Subject's use of the Services • To notify the Data Subjects about changes to the Services • To ensure the security of the Services (e.g. to be alerted of and respond to suspicious login attempts; to assist Syndigo in responding to security incidents) • To analyze traffic patterns in the Services • To cross-reference IP addresses against incoming requests to ensure they do not exceed or abuse contractual expectations. Applicable to Enhanced Content only: • To provide analysis information to Client and its suppliers to evaluate the performance of products and websites using Enhanced Content
The following is deemed an instruction by the Client to Process Client Personal Data in the following manners:	• Processing in accordance with the Agreement; • Processing initiated by Data Subjects in their use of the Services; and • 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.
Nature of Processing Client Personal Data:	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.

	Applicable to Enhanced Content only: - User management and product information performance analytics
Duration of Processing Client Personal Data:	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.
Further Processing:	Syndigo and its Contracted Processors shall not carry out further Processing on Client Personal Data.
Frequency of Transfer of Client Personal Data:	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.
Retention of Client Personal Data by Syndigo:	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.
Syndigo's Technical and Organizational Measures:	Description of the technical, administrative, and organizational security measures implemented by Syndigo can be found at https://syndigo.com/security-and-reliability/.
Subject Matter, Nature, and Duration of Processing by Contracted Processors; Technical and Organizational Measures of Contracted Processors:	The subject matter, nature, and duration of Processing by Contracted Processors is set out in https://syndigo.com/subscription-clients-subprocessors/ Syndigo has a vendor management procedure that includes an exhaustive review of data processing agreements against the requirements of Applicable 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.

Exhibit B

Jurisdiction Specific Terms

1. **Australia**. When applicable, the Processing of Client Personal Data shall be compliant with the Australian Privacy Principles, the Australian Privacy Act (1988), and any other applicable law, regulation, or decree of Australia pertaining to the protection of such information.

2. **Brazil**. When applicable, the Processing of Client Personal Data shall be compliant with Brazil's Lei Geral de Proteção de Dados (Law No. 13.709 of 14 August 2018) and any other applicable law, regulation, or decree of Brazil pertaining to the protection of such information.

3. **Canada.** When applicable, the Processing of Client Personal Data shall be compliant with the Canadian Federal Personal Information Protection and Electronic Documents Act and any other applicable law, regulation, or decree of Canada pertaining to the protection of such information.

4. **European Economic Area.**

4.1. **Definitions.**

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

(b) "**EEA Data Protection Laws**" means the EU GDPR and all laws and regulations of the EU and the EEA countries applicable to the Processing of Client Personal Data.

(c) "**EU GDPR**" (as used in the Addendum) means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as may be amended from time to time.

(d) "**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.

4.2. **Restricted Transfers.**

(a) With regard to any Restricted Transfer subject to EEA Data Protection Laws between the Parties, 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 EU GDPR;

(ii) Syndigo LLC's certification to the EU-U.S. Data Privacy Framework;

(iii) the appropriate Standard Contractual Clauses adopted by the European Commission from time to time; or

(iv) any other lawful data transfer mechanism, as laid down in EEA Data Protection Laws.

4.3. **Standard Contractual Clauses.**

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

(b) The Parties agree that any references to clauses, annexures, modules and choices within this Section shall be deemed to be the same as the cognate and corresponding references within any appropriate, updated Standard Contractual Clauses as may be applicable from time to time pursuant to the Addendum.

(c) For the purposes of the EU 2021 Standard Contractual Clauses and any substantially similar Standard Contractual Clauses which may be adopted by the relevant authorities in the future:

(i) The Parties agree to apply Module Two with respect to Controller-to-Processor Restricted Transfers;

(ii) Clause 7: The Parties choose not to include the optional docking clause;

(iii) Clause 9(a): The Parties choose option 2, “General Written Authorization,” and the time period set forth in Section 6 of the Addendum (The procedures for designation and notification of new Contracted Processors are set forth in more detail in Section 6 of the Addendum);

(iv) Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body;

(v) Clause 13 (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 EU 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).

(vi) Clause 17: The Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland;

(vii) Clause 18: Any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland;

(viii) Annex I (A and B): The content of Annex I(A) and (B) is set forth in Exhibit A;

(ix) Annex II: The content of Annex II is set out https://syndigo.com/security-and-reliability/

(x) Annex III: The content of Annex III is set out https://syndigo.com/subscription-clients-subprocessors/

(d) The terms contained in **Exhibit C** to the Addendum supplement the Standard Contractual Clauses.

(e) In cases where the Standard Contractual Clauses apply and 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 with regard to the Restricted Transfer in question.

5. Switzerland

5.1. **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) "**FDPIC**" means the Swiss Federal Data Protection and Information Commissioner.

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

5.2. **Restricted Transfer.**

(a) With regards to any Restricted Transfer subject to Swiss Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

(i) A valid adequacy decision adopted by the FDPIC on the basis of Article 6 of the FADP;

(ii) Syndigo LLC's certification to the Swiss-U.S. Data Privacy Framework;

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

(iv) The appropriate Standard Contractual Clauses adopted by the FDPIC from time to time; or

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

5.3. **EU 2021 Standard Contractual Clauses.**

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

(b) The Parties incorporate and adopt the EU 2021 Standard Contractual Clauses for Restricted Transfers subject to Swiss Data Protection Laws in the same manner set forth in Section 4.3 of these Jurisdiction Specific Terms, subject to the following:

(i) Clause 13 (Annex I.C): The competent 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;

(ii) Clause 17.The EU 2021 Standard Contractual Clauses shall be governed by the laws of the Swiss Confederation.

(iii) Clause 18: Any dispute arising from the EU 2021 Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland.. The

Parties' selection of forum may not be construed as forbidding Data Subjects habitually resident in Switzerland from suing for their rights in Switzerland;

(iv) 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 are any Restricted Transfers subject to Swiss Data Protection Laws.

(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.

6. United Kingdom

6.1. Definitions.

(a) "**UK Data Protection Laws**" includes the Data Protection Act 2018 and the UK GDPR.

(b) "**UK GDPR**" (as used in the Addendum) 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.

(c) "**UK ICO**" means the UK Information Commissioner's Office.

(d) "**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).

6.2. UK Restricted Transfers:

(a) With regard to any Restricted Transfer subject to UK Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

(i) A valid adequacy regulation pursuant to the requirements under UK Data Protection Laws;

(ii) Syndigo LLC's certification to the UK Extension to the EU-U.S. Data Privacy Framework;

(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.) to the EU 2021 Standard Contractual Clauses; or

(iv) any other lawful data transfer mechanism, as laid down in the UK Data Protection Laws.

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

(i) Table 1: The content of Table 1 of the International Data Transfer Addendum is set out in **Exhibit A**.

(ii) Table 2: The content of Table 2 of the International Data Transfer Addendum is incorporated and adopted as to Restricted Transfers subject to UK Data Protection Laws in exactly the same manner set forth in Section 4.3 of these Jurisdiction Specific Terms, subject to the following changes:

- Clause 13 (Annex I.C): The competent authority shall be the UK ICO.
- Clause 17: The UK International Data Transfer Addendum shall be governed by the laws of England and Wales.
- Clause 18: Any disputes arising from the UK International Data Transfer Addendum shall be resolved by the courts of England and Wales. A Data Subject may also bring legal proceedings against the Data Exporter 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.

(iii) Table 3: The content of Table 3 (Annexes 1A, 1B, II, and III) of the International Data Transfer Addendum is set forth as follows:

- Annex 1A: The Parties' details are found in the Agreement.
- Annex 1B: The description of the transfer is set forth in **Exhibit A**.
- Annex 1C: The technical and organizational measures are set out in **Exhibit A** and in **Exhibit C**.
- Annex III: The list of sub-processors is located at https://www.syndigo.com/subscription/clients/subprocessors/.

(iv) Table 4: The Parties agree that both the Data Importer and the Data Exporter may end 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.

7. United States of America.

7.1. **Applicability**. Wherever the Processing pursuant to the Addendum falls within the scope of United States Data Protection Laws (defined below), the provisions of the Addendum and this Section shall apply to such Processing.

7.2. **Definitions**.

(a) "**United States Data Protection Laws**" include, individually and collectively, enacted state and federal laws, acts, and regulations of the United States of America that apply to the Processing of Client Personal Data and the obligations regarding Personal Data Breaches, as may be amended from time to time. Such laws include, without limitation:

(i) the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 et seq.)., and the California Consumer Privacy Act Regulations, together with all implementing regulations;

(ii) the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq., together with all implementing regulations;

(iii) the Connecticut Act Concerning Data Privacy and Online Monitoring, Pub. Act No. 22015;

(iv) the Utah Consumer Privacy Act, Utah Code Ann. S 13-61-101 et seq.; and

(v) the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-571 et seq.

(b) "**Personal Data Breach**" (as used in the Addendum) includes "**Breach of Security**" and "**Breach of the Security of the System**" as defined under applicable United States Data Protection Laws.

(c) The terms "**Business Purpose**", "**Commercial Purpose**", "**Sell**", and "**Share**" shall have the same meanings as under applicable United States Data Protection Laws, and their cognate and corresponding terms shall be construed accordingly.

7.3. **Processing of Client Personal Data.**

(a) Client discloses Client Personal Data to Syndigo solely for: (i) valid Business Purposes; and (ii) to enable Syndigo to perform the Services.

(b) Syndigo shall not: (i) Sell or Share Client Personal Data; (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 United States Data Protection Laws; (iii) retain, use, or disclose Client Personal Data except where permitted under the Agreement between Client and Syndigo; nor (iv) combine Client Personal Data with other information that Syndigo Processes on behalf of other persons or that Syndigo collects directly from the Data Subject, with the exception of Processing for Business Purposes. Syndigo certifies that it understands these prohibitions and agrees to comply with them.

7.4. **Termination**. Upon termination of the Agreement, Syndigo shall, as soon as reasonably practicable, destroy all Personal Data it has Processed on behalf of Client after the end of the provision of Services relating to the Processing and destroy all copies of the Client Personal Data unless applicable law requires or permits storage of such Client Personal Data.

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.