Syndigo
Jurisdiction Specific Terms for Service Providers

Last updated: August 12, 2025

These Jurisdiction Specific Terms are an integral part of the Syndigo Vendor-Facing Data Processing Addendum ("**Addendum**") entered into between the Parties. By signing the Addendum, the Parties have agreed to comply with these Jurisdiction Specific Terms which apply to the extent that a Party Processes Personal Data originating from or protected by Applicable Data Protection Laws in a jurisdiction identified herein.

The terms and definitions specified in these Jurisdiction Specific Terms shall apply with respect to the applicable jurisdiction in addition to the terms of the Addendum. Capitalized terms which are used but not defined shall have the meaning given to those terms in the Addendum.

1. Argentina

1. Applicability. Wherever the Processing of Syndigo Personal Data pursuant to the Addendum falls within the scope of the Argentine Republic's Personal Data Protection Law 25,326, Regulatory Decree 1558/2001, or any other corresponding decrees, regulations, or guidance governing the Processing of Personal Data in Argentina (collectively "**Argentine Data Protection Laws**"), the provisions of the Addendum and this Section shall apply to such Processing.
2. Restricted Transfers. With regards to any Restricted Transfer subject to Argentine Data Protection Laws between the Parties one of the following transfer mechanisms shall apply, in the following order of precedence:
    a. A valid adequacy decision adopted by the Argentine National Bureau of Personal Data Protection ("**NBPDP**").
    b. The appropriate Standard Contractual Clauses adopted by the NBPDP from time to time.
    c. Any other lawful data transfer mechanism, as laid down in Argentine Data Protection Laws.
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 annexures 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 annexures to Annex II of the Standard Contractual Clauses promulgated by the NDPDP in its Provision 60-E/2016 ("**Argentine SCCs**") and any substantially similar Standard Contractual Clauses which may be adopted by the relevant authorities in the future, the content of Annex A of the Argentine SCCs is set forth in **Exhibit A** of the Addendum.

d. In cases where the Standard Contractual Clauses applies 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.

4. Termination. Upon termination of the Agreement, Service Provider shall destroy all Personal Data it has Processed on behalf of Syndigo after the end of the provision of Services relating to the Processing and destroy all copies of the Personal Data unless applicable law requires or permits storage of such Personal Data.

2. Australia

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

3. Brazil

1. Applicability. Wherever the Processing pursuant to the Addendum falls within the scope of 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 (collectively "**Brazilian Data Protection Laws**"), the provisions of the Addendum and this Section shall apply to such Processing.

2. Restricted Transfers. With regard to any Restricted Transfer subject to Brazilian Data Protection Laws, one of the following transfer mechanisms shall apply, in the following order of precedence:

   a. A valid adequacy decision adopted by the Brazilian Data Protection Authority ("**ANDP**") on the basis of Resolution 19/2024;

   b. The Standard Contractual Clauses adopted by the ANDP from time to time ("**Brazilian Standard Contractual Clauses**");

   c. The recognition of foreign Standard Contractual Clauses that provide an equivalent level of protection as the Brazilian Standard Contractual Clauses by the ANDP; or

   d. Any other lawful data transfer mechanism, as laid down in Brazilian Data Protection Laws, as the case may be.

3. Standard Contractual Clauses.

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

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

   c. For the purposes of the Brazilian Standard Contractual Clauses and any substantially similar Standard Contractual Clauses which may be adopted by the relevant authorities in the future, the Parties agree to apply the following:

      i. Clause 1: The content of Clause 1 is set forth in **Part A of Exhibit A** to the Addendum.
      ii. Clause 2: The content of Clause 2 is set forth in **Part B of Exhibit A** to the Addendum.

iii. Clause 3: The Parties choose Option B. The process for onward transfer is outlined Section 6 in conjunction with in **Appendix II to Exhibit A** of the Addendum.

iv. Clause 4: The Parties choose Option A where Syndigo is the Controller and Service Provider is the Processor; and Option B where Syndigo is the Processor and Service Provider is the Sub-processor for the identification information of the Third-Party Controller.

1. Clause 4.1 (a): The Parties choose Exporter.
2. Clause 4.1 (b): The Parties choose Exporter.
3. Clause 4.1 (c): The Parties choose Exporter.

v. Section III: The content of Annex II is set forth in **Appendix I to Exhibit A** to the Addendum.

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

4. Bulgaria

1. Applicability. Wherever the Processing pursuant to the Addendum falls within the scope of Bulgaria's Personal Data Protection Act (as amended in November 2019), (if ECA applies to the Processing): the Electronic Communications Act, and any other corresponding decrees, regulations, or guidance, the provisions of the Addendum and this Section shall apply to such Processing.

2. General. Service Provider shall:

a. return to Syndigo any Personal Data Processed pursuant to the Addendum within a period of one month after having become aware of any Personal Data that has been disclosed (i) without a legal basis pursuant Article 6 (1) of the EU GDPR, or (ii) contrary to the principles under Article 5 of the EU GDPR; or, if this is impossible or would involve disproportionate efforts, erase or destroy the Personal Data; and

b. if the Personal Data is erased or destroyed in accordance with Section 4.2(a) of these Jurisdiction Specific Terms, document such erasure and destruction.

5. Canada

When applicable, the Processing of Syndigo Personal Data shall be compliant with the Canadian Federal Personal Information Protection and Electronic Documents Act and any other applicable Canadian federal or state law, regulation, or decree of Canada, or its territories therein, pertaining to the protection of such information.

6. Colombia

1. Applicability. Wherever the Processing pursuant to the Addendum falls within the scope of Colombia's Data Protection Law No. 1581 of 2012 ("**Data Protection Law No. 1581**"), Data Protection Decree No. 1377 of 2013 ("**Data Protection Decree**"), and any corresponding decrees, regulations, or guidance (collectively "**Colombian Data Protection Laws**"), the provisions of the Addendum and this Section shall apply to such Processing.

2. General. As applicable, Service Provider shall comply with all requirements applicable to Processors under the Columbian Data Protection Laws, including but not limited to obligations under Article 18 of Data Protection Law No. 1581 and Articles 11, 23, and 25 of the Data Protection Decree. Service Provider shall also comply with Syndigo's Information Processing Policy, if any.

3. The Addendum sets out the additional required contractual elements under Article 25 of the Data Protection Decree, such as the scope of Processing, the activities that Service Provider is authorized to perform on Syndigo's behalf, Service Provider's obligations relative to Syndigo and Data Subjects, and Service Provider's obligations to safeguard the security and confidentiality of Personal Data.

7. European Economic Area

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

2. 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 GDPR and all laws and regulations of the EU and the EEA countries applicable to the Processing of Syndigo Personal Data.

    c. "**EU GDPR**" 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.

3. Restricted Transfers. With regard to any Restricted Transfer subject to EEA Data Protection Laws, one of the following transfer mechanisms shall apply, in the following order of precedence:

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

    b. The appropriate Standard Contractual Clauses adopted by the European Commission from time to time; or

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

4. Standard Contractual Clauses.

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

    b. The Parties agree that any references to clauses, annexures, modules, and choices within the EU 2021 Standard Contractual Clauses 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 the following module[s]:

A. Module Two with respect to Controller-to-Processor Restricted Transfers;

B. Module Three with respect to Processor-to-Sub-Processor Restricted Transfers; and

C. Module Four with respect to Processor-to-Controller Restricted Transfers.

i. Clause 7: The Parties choose not to include the optional docking clause.

ii. Clause 9(a): The Parties choose Option 2, "General Written Authorization," and the time period set forth in Section 6.4 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.

iii. Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.

iv. Clause 13 (Annex I.C): The competent Supervisory Authority is the Irish Supervisory Authority.

v. Clause 17: The clauses shall be governed by the laws of the Republic of Ireland.

vi. Clause 18: The Parties agree that any dispute arising from the EU 2021 Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland.

vii. Annex I(A and B): The content of Annex I(A) is set forth in **Part A of Exhibit A** to the Addendum.

viii. Annex II: The content of Annex II is set forth in **Appendix I to Exhibit A** to the Addendum.

ix. Annex III: The contents of Annex III is set out in **Appendix II to Exhibit A** to the Addendum.

5. The terms contained in **Annex A** to these Jurisdiction Specific Terms supplement the EU 2021 Standard Contractual Clauses.

6. In cases where the EU 2021 Standard Contractual Clauses apply and there is a conflict between the terms of the Addendum and the terms of the EU 2021 Standard Contractual Clauses, the terms of the EU 2021 Standard Contractual Clauses shall prevail with regard to the Restricted Transfer in question.

8. India

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

2. Definitions.

    a. "**Indian Data Protection Laws**" means, once fully in effect, the Digital Personal Data Protection Act, 2023 and the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and any other laws and regulations of India applicable to the Processing of Personal Data.

    b. "**Sensitive Personal Data or Information**" shall have the meaning ascribed to it in Indian Data Protection Laws.

3. Compliance. The Service Provider agrees that its Processing of Syndigo Personal Data shall be compliant with Indian Data Protection Laws.

4. Processing Sensitive Personal Data or Information. Service Provider agrees to only Process Syndigo Personal Data which constitutes Sensitive Personal Data or Information to perform the terms of the Agreement and for no other purpose without the prior written consent of Syndigo. Where Service Provider Processes Syndigo Personal Data that constitutes Sensitive Personal Data or Information, Service Provider may not share, disclose, or transfer any such Sensitive Personal Data or Information to any third party without the prior written consent of Syndigo

5. Security Measures. Service Provider agrees to implement security practices, standards, and procedures specified in Indian Data Protection Laws and agrees to maintain a documented information security program and information security policies throughout the duration of the Addendum.

9. Israel

1. Applicability. Wherever the Processing pursuant to the Addendum falls within the scope of Israel's Protection of Privacy Law (5741-1981), the Protection of Privacy Regulations (Data Security) 5777-2017, and any corresponding decrees, regulations, or guidance (collectively "**Israeli Data Protection laws**"), the provisions of the Addendum and this Section shall apply to such Processing.

2. Deletion or Return of Personal Data. After returning or deleting Syndigo Personal Data pursuant to Section 10 of the Addendum, Service Provider shall provide Syndigo with written confirmation that it no longer possesses any Syndigo Personal Data.

3. General. Service Provider shall notify Syndigo, at least once annually (and in a format to be agreed upon by the Parties), on the manner in which Service Provider has implemented its obligations in the Addendum.

10. Singapore

1. Applicability**.** Wherever the Processing pursuant to the Addendum falls within the scope of Singapore's Personal Data Protection Act 2012, Personal Data Protection (Amendment) Bill 2020, Personal Data Protection Regulations 2021, and any corresponding decrees, regulations, or guidance, the provisions of the Addendum and this Section shall apply to such Processing.

2. Retention of Personal Data. Service Provider shall not retain any Syndigo Personal Data (or any documents or records containing Syndigo Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of the Agreement.

3. Deletion or Return of Personal Data**.** After returning or deleting Syndigo Personal Data pursuant to Section 10 of the Addendum, Service Provider shall provide Syndigo with written confirmation that it no longer possesses any Syndigo Personal Data.

11. Switzerland

1. Applicability. Wherever the Processing pursuant to the Addendum falls within the scope of Swiss Data Protection Laws (defined below), the provisions of the Addendum and this Section shall apply to such Processing.
2. 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 as amended ("**FADP**") and the Ordinance to the Federal Act on Data Protection.
3. Restricted Transfers. With regard 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:
    a. a valid adequacy decision adopted by the FDPIC on the basis of Article 6 of the FADP;
    b. the Standard Contractual Clauses adopted by the FDPIC; or
    c. any other lawful transfer mechanism, as laid down in Swiss Data Protection Laws.
4. Standard Contractual Clauses.
    a. The Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses, which have been adopted for use by the FDPIC with certain modifications. The Parties are deemed to have accepted, executed, and signed the EU 2021 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 7.3 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 clauses shall be governed by the laws of the Republic of Ireland.
        iii. Clause 18: The Parties agree that any dispute arising from the EU 2021 Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland. The Parties' selection of forum may not be construed as forbidding Data Subjects habitually resident in Switzerland from suing for their rights in Switzerland.
5. References to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the FADP and the equivalent articles or sections therein, insofar as there any Restricted Transfers subject to Swiss Data Protection Laws.

6. In cases where the EU 2021 Standard Contractual Clauses apply and there is a conflict between the terms of the Addendum and the terms of the EU 2021 Standard Contractual Clauses, the terms of the EU 2021 Standard Contractual Clauses shall prevail regarding the Restricted Transfer in question.

12. United Kingdom

1. Applicability. Wherever the Processing pursuant to the Addendum falls within the scope of UK Data Protection Laws (defined below), the provisions of the Addendum and this Section shall apply to such Processing.
2. Definitions.
    a. "**UK Data Protection Laws"** includes the Data Protection Act 2018 and the UK GDPR (as defined below).
    b. "**UK GDPR**" means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
    c. "**UK ICO**" means the UK Information Commissioner's Office.
    d. "**UK IDTA**" means the International Data Transfer Agreement issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.
3. Restricted Transfers. With regard to any Restricted Transfer subject to UK Data Protection Laws, one of the following transfer mechanisms shall apply, in the following order of precedence:
    a. A valid adequacy decision adopted pursuant to Article 45 of the UK GDPR;
    b. The UK IDTA; or
    c. Any other lawful data transfer mechanism, as laid down in the UK Data Protection Laws, as the case may be.
4. UK IDTA:
    a. The Addendum hereby incorporates by reference the UK IDTA. The Parties are deemed to have accepted, executed, and signed the UK IDTA where necessary in its entirety.
    b. For the purposes of the tables to the UK IDTA:
    i. Table 1: The information required by Table 1 appears within **Part A of Exhibit A** to the Addendum.
    ii. Table 2:
        A. The UK IDTA shall be governed by the laws of England and Wales.
        B. The Parties agree that any dispute arising from the UK IDTA shall be resolved by the courts of England and Wales.
        C. The Parties' controllership and data transfer roles are set out in **Part A of Exhibit A** to the Addendum.
        D. The Data Importer will inform the Data Exporter whether or not the UK GDPR applies to the Data Importer's Processing of the Personal Data.

E. The Addendum and the Agreement set out the instructions for Processing Personal Data.

F. The Data Importer shall Process Personal Data for the time period set out in **Part B of Exhibit A** to the Addendum. The Parties agree that neither Party may terminate the UK IDTA before the end of such time period by serving one month's written notice.

G. The Data Importer may only transfer Personal Data to authorized Contracted Processors (if applicable), as set out within Section 6 of the Addendum, or to such third parties that the Data Exporter authorizes in writing or within the Agreement.

H. Each Party must review the Addendum at regular intervals, to ensure that the Addendum remains accurate and up to date and continues to provide appropriate safeguards to the Personal Data. Each Party will carry out these reviews as frequently as at least once each year or sooner.

iii. Table 3: The content of Table 3 is set forth in **Part B of Exhibit A** and may be updated in accordance with Section 3.3 of the Addendum.

iv. Table 4: The content of Table 4 is set forth in **Appendix I to Exhibit A** and may be updated in accordance with Section 3.3 of the Addendum.

c. Part 2 (Extra Protection Clauses) and Part 3 (Commercial Clauses) of the UK IDTA are noted throughout the Addendum.

d. The terms contained in **Annex A** to the Addendum supplement the UK IDTA.

e. In cases where the UK IDTA applies and there is a conflict between the terms of the Addendum and the terms of the UK IDTA, the terms of the UK IDTA shall prevail.

13. United States of America

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 the Section shall apply to such Processing.

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 Personal Data, 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 Montana Consumer Data Privacy Act;

v. the Oregon Consumer Privacy Act;

vi. the Texas Data Privacy and Security Act;

vii. the Utah Consumer Privacy Act, Utah Code Ann. S 13-61-101 *et seq.*; and

viii. 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.

3. Processing of Syndigo Personal Data.

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

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

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

Supplemental Clauses to the Standard Contractual Clauses and UK IDTA

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

1. Definitions

1. For the purpose of interpreting this Annex, the following terms shall have the meanings set out below:
    a. "**EO 12333**" means the U.S. Executive Order 12333.
    b. "**FISA**" means the U.S. Foreign Intelligence Surveillance Act.
    c. "**Schrems II Judgment**" means the judgment of the European Court of Justice in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems.

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

1. U.S. Surveillance Laws
    a. Data Importer represents and warrants that, as of the Effective Date, it has not received any national security orders of the type described in Paragraphs 150-202 of the Schrems II Judgment.
    b. Data Importer represents that it reasonably believes that it is not eligible to be required to provide information, facilities, or assistance of any type under FISA Section 702 because:
        i. No court has found Data Importer to be an entity eligible to receive legal process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C. § 1881(b)(4); or (ii) an entity belonging to any of the categories of entities described within that definition.
        ii. If Data Importer were to be found eligible for process under FISA Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to UPSTREAM collection pursuant to FISA Section 702, as described in paragraphs 62 and 179 of the Schrems II Judgment.
    c. EO 12333 does not provide the U.S. government the ability to order or demand that Data Importer provide assistance for the bulk collection of information and Data Importer shall take no action pursuant to EO 12333.
2. Other Surveillance Laws
    a. Data Importer represents and warrants that, as of the Effective Date:
        i. it is not subject to any legislation, nor any executive powers apply in the jurisdiction in which it operates and Processes Syndigo's Personal Data that enable government authorities' access to Data Exporters' Personal Data;
        ii. it has not cooperated with local authorities in n the jurisdiction in which it operates and processes Syndigo's Personal Data to conduct surveillance of communications with

regard to the Personal Data of any of its customers, be it on voluntary or mandatory basis; and

iii. it has not been the subject of a warrant or order under local laws with regard to a request for disclosure of any Personal Data that it stores or otherwise Processes for other companies.

3. Notice of Change

   a. Service Provider agrees and warrants that it has no reason to believe that laws applicable to Service Provider or its Contracted Processors, including in any jurisdiction to which Syndigo Personal Data is transferred either by Service Provider or by a Contracted Processor, prevents Service Provider from fulfilling the instructions received from Syndigo, or performing its obligations under the Addendum.

   b. Service Provider shall monitor any legal, policy, or other developments that might lead to its inability to comply with its obligations under the Addendum. In the event of a change of law that is likely to have a substantial adverse effect on the warranties and obligations provided by the Addendum, Service Provider will promptly notify Syndigo in writing, in which case Syndigo is entitled to (i) suspend the transfer of Syndigo Personal Data, (ii) encrypt the Syndigo Personal Data without provision of the cryptographic key to the Service Provider or any Contracted Processor, (iii) terminate the Addendum, and/or (iv) require the Service Provider to return or delete the Syndigo Personal Data.

3. Backdoors

1. Data Importer certifies that:

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

   b. It has not purposefully created or changed its business processes in a manner that facilitates governmental access to Syndigo Personal Data or systems.

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

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

4. Information About Legal Prohibitions

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

5. Additional Measures to Prevent Authorities from Accessing Syndigo Personal Data

1. Notwithstanding the application of the security measures set forth in the Addendum, Data Importer will implement internal policies establishing that:

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

b. Data Importer's Data Protection Officer or Data Protection Contact Person (as applicable) listed in **Exhibit A** to the Addendum shall be notified upon receipt of each request or order for transferred Syndigo Personal Data;

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

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

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

6. Termination

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