INSTRUCTIONS FOR EXECUTING THIS DATA PROCESSING ADDENDUM

To complete this Data Processing Addendum ("DPA"), you must complete all of the following steps:

1. Complete page two (2) of this document by inserting the full legal name of the Client entity.

2. Complete and sign the signature block for Client on page nine (9).

3. Complete the Standard Contractual Clauses by inputting the Client name, address, signature and any other requested information at the bottom of page 26 for the "Data Exporter"

4. Send the completed and signed DPA to info@southtech.com.

Data Processing Addendum

This Data Processing Addendum ("DPA") supplements and amends the Master Services Agreement, entered into between SouthTech Solutions, Inc. d/b/a SouthTech ("SouthTech") and _____ ("Client") pursuant to which SouthTech is obligated to perform Services for Client (together with any exhibits, schedules and other attachments to such agreement(s), the "Agreement").

1. **Applicability**. This DPA applies to SouthTech if SouthTech will process Personal Information (defined below) in connection with the performance of the Services and Client properly completes the instructions for completing this DPA as set forth on the cover page of this DPA.

2. **Definitions**. For purposes of this DPA, the following definitions shall apply:

"**Applicable Law**" means all applicable laws, statutes, ordinances, cases (common law), constitutions, regulations, treaties, rules, codes, and other pronouncements, as amended and supplemented, that have the effect of law in the United States of America, any foreign country or any domestic or foreign state, country, city, or other political subdivision, including those promulgated, interpreted or enforced by any governmental authority.

"**Authorized Persons**" means the persons or categories of person that Client authorizes SouthTech to provide Personal Information to for processing in accordance with Client's instructions as set forth in the Agreement.

"**Business Purpose**" means the Services described in the Agreement and specifically identified in Appendix A.

"**Data Breach**" means any accidental, unlawful or unauthorized access, acquisition, use, modification, disclosure, loss, destruction of or damage to Personal Information or any other unauthorized processing of Personal Information in violation of the Agreement or this DPA.

"**Data Subject**" means the identified or identifiable natural person who is the subject to the Personal Information.

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, as may be amended or supplemented.

"**Personal Information**" means any information SouthTech processes in accordance with the Agreement that (a) identifies or relates to a data subject who can be identified directly or indirectly from that data alone or in combination with other information in SouthTech possession or control or that SouthTech is likely to have access to, or (b) the data that Applicable Law otherwise defines as protected personal information.

"**Privacy Laws**" means all Applicable Laws relating to the privacy, confidentiality, retention, or security of Personal Information, including, without limitation, the GDPR.

"**processing, processes, or process**" means any activity that involves the use of Personal Information or that relevant Privacy Laws may otherwise include in the definition of processing, processes, or process, including obtaining, recording, storing, or holding the data that contains Personal Information, or carrying out any operation or set of operations on the data containing Personal Information, including, without limitation, organizing, amending, analyzing, retrieving, using, disclosing, Transferring, or destroying such Personal Information.

"**Services**" means the services SouthTech will perform for Client under the Agreement.

"**Standard Contractual Clauses (SCC)**" means the European Commission's standard contractual clauses for the transfer of personal data form the European Union to third countries.

"**Transfer**" or "**Transferring**" means the access by, transfer or delivery to, or disclosure to a person, entity, or system of Personal Information where such person, entity, or system is located in a country or jurisdiction other than the country or jurisdiction from which the Personal Information originated.

3. **Processing**.

a. SouthTech will process Personal Information only on behalf of Client as required to deliver the Services in accordance with the Agreement, including this DPA, and in accordance with Client's instructions as issued in writing. SouthTech acknowledges and agrees that Client is a data controller and SouthTech is a data processor as those terms are defined under applicable Privacy Laws. SouthTech will process Personal Information at all times in compliance with Applicable Law.

b. The subject-matter, the duration of processing, the nature and purpose of the processing, and the types of personal data and categories of data subjects are set forth in the Agreement and summarized in Appendix A.

c. Client shall retain control over the Personal Information for the duration that this DPA is in effect and is responsible for its compliance obligations under the applicable Privacy Laws, including providing any required notices and obtaining any required consents, and for the processing instructions that it provides to SouthTech.

d. SouthTech is prohibited from processing Personal Information in a manner that is not in accordance with Client's instructions, except which any variation is in writing and executed by duly authorized representatives of both Client and SouthTech. If Applicable Law requires SouthTech to engage in processing that is or could be construed to be inconsistent with Client's instructions, then SouthTech must promptly notify Client and will not commence such processing, unless Applicable law prohibits such notice. In the event that SouthTech believes any instruction provided by Client hereunder violates or could result in processing in violation of Applicable Law, then SouthTech will notify Client immediately.

4. **SouthTech's Obligations**.

a. SouthTech will only process, retain, use, or disclose Personal Information to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with Client's written instructions as detailed in the Agreement and more specifically in Appendix A. SouthTech will not process, retain, use, or disclose the Personal Information for any other purpose or in a manner that does not comply with this DPA or applicable Privacy Laws.

b. SouthTech shall comply with any Client request or instruction, requiring SouthTech to amend, Transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized processing; provided, however, that SouthTech shall have no such obligation to the extent that Client has access to the Personal Information and functionality to carry out the same activity without intervention from SouthTech (including, but not limited, to file level control).

c. SouthTech shall maintain the confidentiality of all Personal Information, will not sell or disclose such Personal Information to any third parties unless specifically authorized by Client, this DPA, or required by law. In the event that an Applicable Law requires SouthTech to process or disclose Personal Information, SouthTech must first inform Client of the legal requirement and provide Client an opportunity to object or challenge the requirement, unless providing notice is prohibited by Applicable Law.

d. SouthTech shall provide its reasonable assistance to Client with meeting the Client's compliance obligations under applicable Privacy Laws, taking into account the nature of SouthTech's processing and the information available to SouthTech.

e. Client acknowledges and agrees that SouthTech is not under any duty to investigate the completeness, accuracy, or sufficiency of any specific Client instruction or the Personal Information other than as specifically required under applicable Privacy Laws.

f. SouthTech will provide notice to Client if SouthTech becomes aware of any changes to the Privacy Laws that may adversely impact SouthTech's performance under the Agreement.

5. **SouthTech's Personnel**.

a. SouthTech will limit access to Personal Information to those of SouthTech's employees who require access to the Personal Information for their job function and in connection with SouthTech's obligations under this DPA and the Agreement.

b. SouthTech will ensure that all of its employees who require access to Personal Information of Client are: (i) informed of its confidential nature and use restrictions; (ii) have undergone training on the applicable Privacy Laws as it concerns handling Personal Information; and (iii) are aware of both SouthTech's duties and their personal duties and obligations under the Privacy Laws and this DPA.

c. SouthTech will take reasonable steps to ensure the reliability, integrity, and trustworthiness of all of its employees having access to the Personal Information.

6. **Security**.

a. SouthTech shall implement and maintain appropriate technical and organizational measures designed to safeguard Personal Information against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution and against accidental loss, destruction, or damage. SouthTech must document the measures it takes in compliance with this Section and periodically review them, at least annually, to ensure they are current and complete.

b. SouthTech shall take reasonable precautions to preserve the integrity of any Personal Information in processes and to prevent any corruption or loss of the Personal Information.

7. **Data Breach and Loss of Personal Information**.

a. In the event that any Personal Information is lost or destroyed, or becomes damaged, corrupted, or unusable, SouthTech will promptly notify Client.

b. SouthTech shall immediately notify Client if SouthTech becomes aware of: (i) any unauthorized or unlawful processing of Personal Information in violation of this DPA; or (ii) any Data Breach.

c. Following the discovery of an occurrence of either Section 7(b)(i) or (ii), SouthTech shall promptly investigate the matter. SouthTech shall provide its reasonable cooperation to Client, including, by providing Client with information regarding:

i. The nature of the Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

ii. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

iii. A description of the likely consequences of the Data Breach;

iv. A description of the measures taken or proposed to be taken by SouthTech, to the extent the Data Breach concerns a system within SouthTech's possession, custody, or control, including, where appropriate, measures to mitigate possible adverse effects.

d. Except as otherwise required by Applicable Laws, SouthTech will not inform any third party of a Data Breach without first obtaining Client's prior written consent.

e. SouthTech agrees that Client shall have the sole right to determine:

i. whether to provide any notification of the Data Breach to any Data Subjects, regulators, law enforcement agencies, or others, as required by law, or regulation or in the Client's discretion, including the content and delivery method chosen to deliver such notice; and

ii. whether Applicable Law requires offering Data Subjects any type of remedy and the nature and extent of such remedy.

8. **Transfer of Personal Information Cross-Border**.

a. Where Privacy Laws restrict the cross-border Transfers of Personal Information, Client shall only Transfer Personal Information to SouthTech as follows:

i. if Client has provided all legally required notice to and obtained consent from the Data Subject to the Transfer in accordance with applicable Privacy Laws; or

ii. the Transfer otherwise complies with applicable Privacy Laws.

b. In the event that any Transfer of Personal Information between SouthTech and the Client requires execution of the Standard Contractual Clauses in order to comply with applicable Privacy Laws, the parties shall complete all relevant details in, and execute the SCC's, which are attached hereto in Appendix B, and take all other actions required to legitimize the Transfer.

c. SouthTech shall not Transfer any Personal Information to another country unless such Transfer complies with the Privacy Laws.

9. **Subcontractors**.

a. SouthTech may only authorize a subcontractor to process Personal Information if:

i. Client is given an opportunity to object within thirty (30) days after SouthTech supplies Client with details regarding the proposed subprocessor;

ii. SouthTech enters into a written contract with the subprocessor that contains terms that are substantially the same as those set forth in this DPA, and upon the Client's request, provides the Client with copies of such contracts; provided, however, that SouthTech may redact commercially sensitive terms;

iii. SouthTech maintains control over all Personal Information it provides to the subprocessor; and

iv. SouthTech remains liable for any act, omission, or breach of this DPA by a subprocessor.

b. A list of SouthTech's subprocessors are provided in Annex III to Appendix B and include any subprocessors name, location, and the person responsible for privacy and data protection compliance.

c. Upon Client's written request, SouthTech shall audit its subprocessor's compliance with its obligations regarding the Client's Personal Information and provide Client with the audit results.

10. **Data Subject Requests; Complaints**.

a. SouthTech shall promptly notify Client if SouthTech receives a request from a Data Subject for access to or deletion of Personal Information, to the extent SouthTech can reasonably determine that the Data Subject's Personal Information was collected by Client.

b. SouthTech will provide Client its cooperation and assistance responding to any complaint, notice, communication, or Data Subject request concerning Personal Information.

c. SouthTech shall not disclose Personal Information to any Data Subject or to a third party unless the disclosure is either at Client's request or instruction, permitted by this DPA, or otherwise required by Applicable Laws.

11. **Term and Termination**.

a. This DPA shall remain in full force and effect for so long as: (i) the Agreement is in full force and effect between SouthTech and Client; or (ii) SouthTech retains any Personal Information related to the Agreement (the "Term").

b. Any provision of this DPA that expressly or by implication is to continue in force and effect after the expiration or termination of this Agreement shall remain in full force and effect.

c. A failure by either SouthTech or Client to comply with the terms of this DPA shall constitute a material breach of this DPA and the Agreement. If either party commits a breach of this DPA, then the other party may terminate the Agreement effectively immediately with written notice to the breaching party and without prejudice to any rights or remedies that the non-breaching may have against the breaching party.

d. In the event that a change in the Privacy Laws prevents either party hereto from fulfilling any part of or all of its obligations under the Agreement, the parties shall suspend the processing of Personal Information until the processing complies with the new requirements under the Privacy Laws. If the parties are unable to bring the Personal Information processing into compliance with the Privacy Laws within thirty (30) days after such change to the Privacy Laws goes into effect, either party may terminate the Agreement with written notice to the other party.

12. **Return of Personal Information**.

a. Upon Client's request, SouthTech shall provide Client a copy of or access to Client' Personal Information within its possession, custody, or control in the format reasonably agreed upon between the parties.

b. On the earlier of (i) expiration of the Agreement; or (ii) termination of the Agreement; SouthTech shall securely destroy or, if directed in writing by Client, return and not retain, all Personal Information related to this DPA in its possession, custody, or control; provided that SouthTech may retain one copy of any Personal Information to the extent SouthTech is legally required to retain such information and only for so long as such requirement exists.

c. If any law, regulation, or government or regulatory body requires SouthTech to retain any documents or materials that SouthTech would otherwise be required to return or destroy, it will notify Client in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends. SouthTech may only use this retained Personal Information for the required retention reason.

13. **Records**.

a. SouthTech will maintain records regarding the processing of Personal Information it carries out for Client, including, but not limited to, the access, control, and security of the Personal Information, approved subcontractors and affiliates, and any other records required by applicable Privacy Laws (the "Records").

b. SouthTech will provide Client with the Records to help enable Client to verify SouthTech's compliance with the obligations under this DPA.

14. **Audits**.

a. At least once per year, SouthTech will conduct site audits of its Personal Information processing practices and information technology and security controls for all facilities and systems used to comply with its obligations under this DPA, including, without limitation, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on industry best practices.

b. Upon Client's written request, SouthTech will make all of the relevant audit reports available for Client to review. All such audit reports shall be classified and handled by Client as Confidential Information under the Agreement.

c. SouthTech shall promptly address any issues, concerns, or exceptions noted in the audit reports with the development and implementation of a corrective action plan by SouthTech's management.

15. **Miscellaneous**. The provisions contained in the Agreement for governing law, dispute resolution, indemnification and liability are incorporated by reference in this DPA.

IN WITNESS WHEREOF, the parties hereto have caused their duly authorized representatives to execute this DPA as of the date noted below.

SOUTHTECH SOLUTIONS, INC. _____**("CLIENT")**

By:_____ Signature:_____

Its:_____ Print Name:_____

Date:_____ Title:_____

Date:_____

List of Appendices

Appendix A: Details of Processing
Appendix B: Standard Contractual Clauses
Annex I: Processing Details
Annex II: Technical and Organizational Measures to Ensure the Security of Data
Annex III: List of Subprocessors

APPENDIX A – Details of Processing

Nature and Purpose of Processing

SouthTech will process Personal Information as necessary to carry out to Services set forth in the Agreement and as Client may update from time to time through written instructions issued pursuant to the DPA.

Duration of Processing

SouthTech will process Personal Information for the Duration of the Agreement as set forth in therein.

Categories of Data Subjects

Client has the option to provide SouthTech with Personal Information through the Services in Client's sole discretion. The Personal Information that is provided to SouthTech may relate to the following categories of Data Subjects:

customers, clients, prospective customers and clients, vendors, business partners, service providers, contact persons for any of the foregoing, Client's employees, agents, representatives, and independent contractors.

Types of Personal Information

Client has the option to submit Personal Information to the Services as it deems appropriate or advisable at Client's sold discretion, which may include the following categories of Personal Information:

name, occupation or title, employer name, contact information for the Data Subject, professional details, personal details, and location information.

Special Categories of Data (if appropriate)

Subject to the requirements contained in the DPA, Client may choose, at Client's sole discretion, to submit data that includes "special categories of personal data" as that term is defined under the GDPR, which includes information revealing details about racial and ethnic origin, political opinions, philosophical and religious beliefs, trade-union membership, and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health, a natural person's sex life, or sexual orientation.

APPENDIX B –
Standard Contractual Clauses
Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

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

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

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

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

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

Clause 2

Effect and invariability of the Clauses

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

not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

(a)

An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b)

Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c)

The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that

prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to

notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data

exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

MODULE TWO: Transfer controller to processor

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

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

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

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

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

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

(g)

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

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a)

Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b)

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

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

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

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

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

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

Clause 15

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

MODULE TWO: Transfer controller to processor

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

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

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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

(b) The Parties agree that those shall be the courts of _____ (specify Member State).

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

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

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1.

Name:_____

Address:_____

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

Activities relevant to the data transferred under these Clauses:_____
_____

Signature and date:_____

Role (controller/processor):_____

2.

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1.

Name: SouthTech Solutions, Inc. dba SouthTech
Address:_____

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

Activities relevant to the data transferred under these Clauses: Data Importer is a provider of technology services, including hosted services solutions for businesses, including the Data Exporter

Signature and date:_____

Role (controller/processor): Processor

2.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Customers, clients, prospective customers and clients, vendors, business partners, service providers, contact persons for any of the foregoing, employees of the client or customer, agents, representatives, and independent contractors.

Categories of personal data transferred

Contact information, occupation or title, employer name, professional details, personal details, and location information

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

_____

_____

_____

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

Personal Data will be transferred on a continuing basis.

Nature of the processing

The nature of the processing is set forth in the Agreement between the parties. The Data Exporter is a provider of technology services, including hosted services for its customers and clients, which

includes storing, structuring, analyzing, computing, and transferring data in accordance with the commands, functions, settings, and instructions of the Data Exporter's clients and customers.

Purpose(s) of the data transfer and further processing

Data Exporter processes personal data hereunder in connection with offering technology services, including hosted services for its customers and clients.

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

Any personal data provided hereunder will be retained and processed for so long as the customer or client decides to place such data within the technology service and any such data will be returned or destroyed upon the earlier to occur of: (i) a request from the client or customer; (ii) expiration or the Agreement; or (iii) termination of the Agreement.

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

_____

_____

_____

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

_____

_____

_____

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

_____
_____
_____
_____

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

_____
_____
_____

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1.

Name:_____
Address:_____

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): _____

2.

Name:_____
Address:_____

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): _____