Instructions

This Data Processing Agreement ("**DPA**") forms part of the service agreement (or other such written or electronic agreement addressing the same subject matter as defined below) ("**Agreement**") between Customer (or its affiliates) and the service provider.

This DPA reflects the parties' agreement with regard to the Processing of Personal Data and applies when Customer acts as Data Controller or as Data Processor and instructs the Data Processor to process personal data of individuals on its behalf or on behalf of its customers.

This DPA consists of:

(i) Data Processing Agreement that sets out the terms and conditions applicable to Processing of Personal Data;
(ii) Schedule 1 - Details of Processing;
(iii) Schedule 2 - Technical and Organizational Measures; and
(iv) Exhibit 1 - Standard Contractual Clauses
(v) Exhibit 2 - UK GDPR International Data Transfer Addendum

Data Processing Agreement

This Data Processing Agreement ("**DPA**") is incorporated into any existing and currently valid Subscription Services Agreement or Terms and Conditions (the "**Agreement**") either previously or concurrently made between you (together, with any subsidiaries and affiliated entities, collectively, "**Customer**") and AVOXI, Inc. ("**Data Processor**"), collectively known as the "Parties" and individually known as a "Party".

1. Subject Matter

1.1 The Parties have entered into an Agreement in relation to the Data Processor providing telecommunications and/or call center software services to the Customer. This DPA applies to the processing of personal data by the Data Processor in accordance with the scope of the Agreement that is subject to the Data Protection Laws (as defined in Clause 1.2 below). In other words, this DPA sets forth additional terms that apply to the extent any information Customer provides to Data Processor pursuant to the Agreement includes Personal Data (as defined below). This DPA shall come into effect on the effective date of the Agreement and the term of this DPA shall correspond to the term of the Agreement. This DPA forms part of and is incorporated into the Agreement, and except as modified below, the terms of the Agreement shall remain in full force and effect. In the event of any inconsistency between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail.

1.2 Unless otherwise defined herein, the following definitions shall apply:

"Data Protection Laws" shall mean (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("**General Data Protection Regulation**" or "**GDPR**"), and (ii) to the extent applicable to the Parties, data protection laws of any other country.

"Personal Data" shall mean any information relating to an alive person, which enables the identification of such person, whether directly or indirectly, and being processed by the Data Processor for performance of the Agreement.

"Processing, process, processed, processes" shall mean any collection, use, disclosure and/or other operation or set of operations which is performed on Personal Data or on sets of Personal Data.

1.3 All capitalized terms that are not expressly defined in this DPA will have the meanings given to them in the Agreement.

2. Processing

2.1 An overview of the categories of the Personal Data, the categories of data subjects, and the nature and purposes for which the Personal Data are being processed by the Data Processor on behalf of the Customer are specified in *Schedule 1* and ANNEX I to the Standard Contractual Clauses.

2.2 The Data Processor shall process Personal Data on behalf of the Customer and in accordance with its documented instructions, for the sole purpose of performing its obligations under the Agreement or as otherwise reasonably instructed by the Customer, and not for the Data Processor's own purposes or other

commercial exploitation, and always in compliance with all applicable Data Protection Laws. If the Data Processor believes an instruction violates the Data Protection Laws, the Data Processor shall inform the Customer without undue delay.

2.3 At any time during the term of this DPA at the Customer's request or upon the termination or expiration of the Agreement, the Data Processor shall promptly return to the Customer all copies, whether in written, electronic or other form or media, of the Personal Data in its possession, or securely dispose of all such copies, and certify in writing to the Customer that such Personal Data has been returned or disposed of securely within 7 days of the request. The Data Processor shall comply with all directions provided by the Customer with respect to the return or disposal of the Personal Data. The Data Processor shall notify all third parties supporting its own processing of the Personal Data of the termination of the DPA and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Customer, at the discretion of the Customer. This DPA shall remain in force until the termination of the Personal Data processing and the erasure of the data by the Data Processor and any sub-processors.

3. Confidentiality and Technical and Organizational Measures

3.1 Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality. This confidentiality obligation shall survive the termination of the DPA.

3.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the processing of the Personal Data appropriate to the risk. Measures shall include, as appropriate, measures for protection against unauthorized or unlawful processing, against accidental, unauthorized or unlawful loss, access to, use, alteration, correction, disclosure, or destruction of the Personal Data, and measures to ensure confidentiality and integrity of the Personal Data.

3.3 The Data Processor shall regularly monitor its compliance with the respective technical and organizational measures, the Data Protection Laws, and accepted industry standards or practices, and will verify this monitoring upon the Customer's request. The Data Processor shall not materially decrease the overall security measures during the term of the Agreement.

4. Information and Audit

4.1 The Data Processor shall make available to the Customer on request all information necessary to demonstrate compliance with this DPA and the Data Protection Laws, and shall allow for audits, at Customer's sole expense, including on-site inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Personal Data. Customer agrees that if it exercises this right, then it will provide Data Processor no less than sixty (60) days advance written notice.

4.2 Upon the Customer's written request, the Data Processor shall make available to the Customer details of technical and organizational measures implemented, all sub-processors engaged, and a copy of the Data Processor's then most recent third-party audits or certifications, as applicable.

4.3 To the extent applicable and required, the Data Processor will, at Customer's expense and taking into account the nature of the Processing and the information available, provide the Customer with cooperation and assistance in relation to any data protection impact assessment or regulatory consultation that the Customer is legally required to make.

5. Sub-processors

5.1 The Data Processor shall not subcontract any of its Service-related activities consisting (partly) of the processing of the Personal Data or requiring Personal Data to be processed by any third party without the prior written authorization of the Customer. The Customer's consent to the engagement of specific sub-processors, if applicable, shall be specified in *Schedule 1* and Exhibit 1.

5.2 The Data Processor shall enter into a written agreement with each sub-processor on terms which offer at least the same level of protection for the Customer's Personal Data as those set out in this DPA prior to the sub-processor's processing any Personal Data, and ensure that the relevant obligations (including but not limited to the information and audit rights) can be directly enforced by the Customer against the Data Processor's sub-processors.

5.3 The Data Processor remains responsible for its sub-processors and fully liable for their acts and omissions as for its own acts and omissions and any references to the Data Processor's obligations, acts and omissions in this DPA shall be construed as referring also to the Data Processor's sub-processors.

5.4 The Data Processor shall inform the Customer of any new sub-processors the Data Processor intends to engage to process the Personal Data. The Customer may object to the engagement of any new sub-processor but shall not unreasonably withhold its consent to such appointment.

5.5 The Data Processor shall ensure that the sub-processor is bound by data protection obligations compatible with those of the Data Processor under this DPA, shall supervise compliance thereof, and must in particular impose on its sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Data Protection Laws.

6. Data Subject Rights

6.1 The Data Processor shall assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Controller' obligations, as reasonably understood by the Customer, to respond to requests to exercise data subject rights under the Data Protection Laws.

6.2 The Data Processor shall promptly notify the Customer of any data subjects' requests or complaints regarding Personal Data within three days from the date it receives such requests or complaints. The Data Processor shall not respond to such requests or complaints except on the documented instructions of the Customer or as required by applicable laws to which the Data Processor is subject, in which case the Data Processor shall inform the Customer of that legal requirement before responding to the request. The Data Processor shall upon the Customer's request provide reasonable efforts to assist the Customer in responding to such data subject's request or complaint.

6.3 If a data subject or a supervisory authority brings a claim against the Customer for damages suffered in relation to the Data Processor's breach of this DPA or Data Protection Laws, the Data Processor shall indemnify the Customer and its affiliates and their respective directors, officers, employees, agents and

subcontractors, from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third party claims against the Customer, its affiliates and their respective directors, officers, employees, agents and subcontractors arising out of or resulting from the Data Processor's failure to comply with any of its obligations under this DPA and/or the Data Protection Laws.

7. Incidents

7.1 When the Data Processor becomes aware of an incident that has a material impact on the Processing of the Personal Data that is the subject of the Agreement, it shall promptly notify the Customer about the incident, shall at all times cooperate with the Customer, and shall follow the Customer's instructions with regard to such incidents, in order to enable the Data Controller to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.

7.2 The term "incident" used in Article 7.1 shall be understood to mean in any case:

(a) a complaint or a request with respect to the exercise of a data subject's rights under the Data Protection Laws.

(b) an investigation into or seizure of the Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent.

(c) any accidental, unauthorized or unlawful loss, access to, use, alteration, disclosure, destruction, or any form of unlawful processing of the Personal Data.

(d) any breach of the security and/or confidentiality as set out in Article 3 of this DPA leading to the accidental, unauthorized or unlawful loss, access to, use, alteration, disclosure, or destruction of the Personal Data, or any indication of such breach having taken place or being about to take place.

(e) where, in the opinion of the Data Processor, implementing an instruction received from the Customer would violate applicable laws to which the Customer or the Data Processor are subject.

7.3 The Data Processor shall at all times have in place written procedures which enable it to promptly respond to the Customer about an incident. Where the incident may require a data breach notification by the Customer under the Data Protection Laws, the Data Processor shall implement its written procedures in such a way that it is in a position to notify the Customer without undue delay after the Data Processor becomes aware of such an incident, and in no event later than 48 hours, after becoming aware of an incident. Such notification shall as a minimum:

(a) describe the nature of the incident, the categories and numbers of data subjects and Personal Data records concerned;
(b) communicate the name and contact details of the Data Processor's data protection officer or other relevant contact from whom more information may be obtained;
(c) describe the likely consequences of the incident;
(d) describe the measures taken or proposed to be taken to address the incident including, where appropriate, measures to mitigate its possible adverse effects; and
(e) other details as may be required by the Data Protection Laws or the supervisory authorities.

7.4 The Data Processor will not disclose to any third party of any incident without obtaining the Customer's prior written approval, except as required by applicable laws to which the Data Processor is subject, in which case the Data Processor shall inform the Customer of that legal requirement before the disclosure.

8. Representations and Warranties

The Data Processor represents and warrants that:

(a) it and anyone operating on its behalf shall only process Personal Data pursuant to the lawful instruction given by the Customer;

(b) it provides and, at all times, maintains appropriate security measures for preventing accidental, unauthorized or unlawful loss, access to, use, alteration, correction, disclosure, or destruction of Personal Data;

(c) it complies with the DPA and the applicable Data Protection Laws; and

(d) its respective directors, officers, employees, agents, sub-processors, subcontractors, and/or any other persons who need to access the Personal Data on its behalf for performing its obligations under the Agreement are reliable and trustworthy and have received the required training on the Data Protection Laws.

9. Indemnification

The Data Processor shall indemnify the Customer from and against all damages, including reasonable attorneys' fees, arising out of or resulting from any third party claims against the Customer arising out of or resulting from Data Processor's willful failure to comply with any of its obligations under this DPA.

10. Severance

Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

11. Amendment and Waiver

No provision of this DPA may be amended, waived or otherwise modified except by an instrument in writing duly executed by authorized representatives of the Parties. The failure or delay of a Party in exercising any rights under this DPA on any occasions shall not be considered a waiver by or deprive the Party of the right thereafter to exercise such right or any other right under this DPA.

12. Governing Law and Jurisdiction

This DPA shall be governed by the laws of the state of Georgia, United States and subject to the exclusive jurisdiction of the courts of the state of Georgia, U.S.A.

13. Counterparts

This DPA may be executed in counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same document. Delivery of an executed signature page to this DPA by facsimile or electronic means (e.g. e-mail, PDF) shall be effective to the same extent as if such party had delivered a manually executed counterpart.

Schedule 1- Details of Processing

1. Personal Data

Types of Personal Data that will be processed in accordance with the scope of the Agreement are those set forth in ANNEX I to the Standard Contractual Clauses.

2. List of authorized sub-processors

The Customer shall on commencement of this Data Processing Agreement approve the engagement of the following sub-processors located within Data Processor's privacy policy found at https://www.iubenda.com/privacy-policy/8179510/full-legal

3. Contact information

Contact information of the Customer

Email: the Customer's email address set out in the Agreement

Address: the Customer's address set out in the Agreement

Contact information of the Data Processor.

Weston Edmunds, EVP
300 Galleria Parkway, Suite 1040, Atlanta, Georgia 30339 U.S.A.
+1.678.348.5042
privacy@avoxi.com or Weston.edmunds@avoxi.com

Schedule 2 - Technical and Organizational Measures

Organizational Controls			
1.	Data Processor has designated a data protection officer (or a person responsible for ensuring compliance with data protection requirements if a data protection officer is not required by law).	☒Yes ☐No	If no please explain:
2.	Data Processor has a formal Data Privacy/Information Security policy, and procedures that cover storage, access and/or transmission of customer data, including records containing personal data?	☒Yes ☐No	If no please explain:
3.	Data Processor's Data Privacy/Information Security policy is reviewed at least annually and amended as Data Processor deems reasonable to maintain protection of Personal Data.	☒Yes ☐No	If no please explain:
4.	Data Processor's employees and any others performing work on Data Processor's behalf are required to sign confidentiality and non-disclosure agreements.	☒Yes ☐No	If no please explain:
5.	Data Processor's employees and any others performing work on Data Processor's behalf receive appropriate data security awareness and training, at least annually.	☒Yes ☐No	If no please explain:
6.	Data Processor undertakes regular audits to ensure its compliance with data protection requirements.	☒Yes ☐No	If no please explain:
7.	Has Data Processor undergone third-party audit certification against the PCI DSS 3.2.1 standard?	☒Yes ☐No	If no please explain:
Physical Access Control			
8.	Data Processor prevents unauthorized individuals from gaining access to the Data Processor's premises.	☒Yes ☐No	If no please explain:
9.	Data Processor restricts access to data centres/rooms where data servers are located.	☒Yes ☐No	If no please explain:
10.	Data Processor uses video surveillance and intrusion detection devices to monitor access to data processing facilities.	☒Yes ☐No	If no please explain:
11.	Data Processor ensures that individuals who do not have access authorization (e.g. technicians, cleaning personnel) are accompanied when accessing data processing facilities.	☒Yes ☐No	If no please explain:

12.	Data Processor stores physical media containing personal data in secured areas.	☒Yes ☐No	If no please explain:
13.	Data Processor ensures secure disposal of documents containing personal data.	☒Yes ☐No	If no please explain:
	System Access Control		
14.	Data Processor ensures that access to systems is supported by an authentication system.	☒Yes ☐No	If no please explain:
15.	Data Processor provides dedicated user IDs for authorized personnel accessing data processing systems for authentication purposes.	☒Yes ☐No	If no please explain:
16.	Data Processor ensures that all data processing systems are password protected to prevent unauthorized persons accessing any personal data.	☒Yes ☐No	If no please explain:
17.	Data Processor has implemented a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password, and requires the regular change of passwords.	☒Yes ☐No	If no please explain:
18.	Data Processor maintains technical measures enforcing timeout of inactive sessions and lockout of accounts after multiple sequential failed login attempts.	☒Yes ☐No	If no please explain:
19.	Data Processor grants data access only to authorized personnel and assigns only the minimum data permissions necessary for those personal to fulfil their duties.	☒Yes ☐No	If no please explain:
20.	Data Processor implements a proper procedure to deactivate user accounts when a user leaves.	☒Yes ☐No	If no please explain:
	System Security		
21.	Data Processor implements controls to use only authorized business equipment to perform the services.	☒Yes ☐No	If no please explain:
22.	Data Processor has implemented network firewalls to prevent unauthorised access to systems and services.	☒Yes ☐No	If no please explain:
23.	Data Processor encrypts personal data at rest.	☒Yes ☐No	If no please explain:
24.	When allowing the use of any removable media, Data Processor enforces encryption on such media.	☒Yes ☐No	If no please explain:

25.	Data Processor ensures that each system used to process personal data runs an up to date malware and antivirus detection and removal solution.	☒Yes ☐No	If no please explain:
26.	Data Processor has measures in place to prevent use/installation of unauthorized hardware and/or software.	☒Yes ☐No	If no please explain:
27.	Data Processor performs penetration testing and vulnerability assessments at least annually.	☒Yes ☐No	If no please explain:
28.	Data Processor enlists a qualified independent third-party to perform penetration testing at least annually.	☒Yes ☐No	If no please explain:
29.	Data Processor remediates identified vulnerabilities or noncompliance with its security configuration requirements.	☒Yes ☐No	If no please explain:
30.	Data Processor has established rules for the safe and permanent destruction of data that are no longer required.	☒Yes ☐No	If no please explain:
	Incident Management		
31.	Data Processor creates back-up copies of personal data, which are stored in protected environments.	☒Yes ☐No	If no please explain:
32.	Data Processor has the ability to restore personal data from those back-ups.	☒Yes ☐No	If no please explain:
33.	Data Processor regularly performs testing of contingency plans or business recovery strategies.	☒Yes ☐No	If no please explain:
34.	Data Processor has an incident response plan to respond to a personal data breach.	☒Yes ☐No	If no please explain:
35.	Data Processor regularly tests the incident response plan, including to respond to a personal data breach	☒Yes ☐No	If no please explain:
36.	Data Processor has a plan to communicate information security incidents or breaches to Data Processor's clients.	☒Yes ☐No	If no please explain:

EXHIBIT 1

STANDARD CONTRACTUAL CLAUSES FOR PERSONAL DATA TRANSFERS TO THIRD COUNTRIES
(MODULE TWO: CONTROLLER-PROCESSOR AND MODULE THREE: PROCESSOR-PROCESSOR)

This Exhibit 1 is part of the DPA and must be included as part of and signed with the DPA to be valid and legally binding.

The Parties shall be deemed to enter into the Controller to Processor Standard Contractual Clauses (Module Two); and into the Processor to Processor Standard Contractual Clauses (Module Three).

The Parties further agree that for the purpose of transfer of Personal Data between the Customer (Data Exporter) and the Company (Data Importer), the following shall apply:

1. Clause 7 of the Standard Contractual Clauses is applicable.
2. In Clause 9, option 2 shall apply.
3. In Clause 11, data subjects may also lodge a complaint with an independent dispute resolution body (i)
4. In Clause 17, OPTION 1 shall apply and that Member State shall be the Republic of Ireland.
5. In Clause 18(b) the Parties choose the courts of Republic of Ireland as their choice of forum.

The Parties shall complete Annexes 1-2 below, which are incorporated in the Standard Contractual Clauses by reference.

APPENDIX

ANNEX I

A. LIST OF PARTIES

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]*
Name: Customer

Address: the Customer's address set out in the Agreement

Registration number: the Customer's registration number as set out in the Agreement or order form

Contact person's name, position and contact details: the Customer's contact details as set out in the Agreement or order form

Activities relevant to the data transferred under these Clauses: The activities specified in the Agreement.

Signature and date: Customer is deemed to have signed this Annex I by accepting AVOXI's Terms and Conditions and/or by signing the Subscription Services Agreement

Role (controller/processor): controller and processor

2. …

Data importer(s):
Name: AVOXI, Inc.

Address: 300 Galleria Parkway, Suite 1040, Atlanta, Georgia 30339, U.S.A.

Contact person's name, position and contact details: Weston Edmunds, EVP

_privacy@avoxi.com;Weston.edmunds@avoxi.com / +1.770.937.9735

Activities relevant to the data transferred under these Clauses:

Performance of the Services pursuant to the Agreement and as further

described in related documentation.

Signature and date: AVOXI is deemed to have signed this Annex I by accepting AVOXI's Terms and Conditions and/or by signing the Subscription Services Agreement

Role (Controller/Processor): Processor

2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The categories of data subjects whose personal data may be processed in connection with the Services are determined and controlled by the data exporter in its sole discretion and may include but are not limited to:

- Customers, contacts and prospects of data exporter;
- Contact details of employees or of contractors of data exporter's customers and prospects;
- Contact details of employees and contractors of data exporter

Categories of personal data transferred

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name;
- Employer;
- Professional title;
- Position;
- Contact information (e.g., email, phone, physical business address);
- Call detail records;
- Call voice recordings (if call recording feature is enabled);
- IP address;
- Device identification data
- Passport number (if required to provision certain virtual telephone numbers)

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.

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Special categories of data would only be processed by Data importer if data exporter is required to provide a passport which is required for particular virtual telephone numbers or if it enables call recording. If so, call recordings are restricted to certain categories of Data importer employees and the call recordings are encrypted at rest.

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

Continuous basis depending on the use of the Services by Customer.

Nature of the processing

The nature of the Processing is the performance of the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

AVOXI will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in related documentation, if applicable, and as further instructed by Customer in its use of the Services.

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

AVOXI will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

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

As per the *"Purpose(s) of the data transfer and further processing"* above, the Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. The Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Identities of the Sub-processors used for the provision of the Services and their country of location are listed in the AVOXI privacy policy found at https://www.iubenda.com/privacy-policy/8179510/full-legal.

C. COMPETENT SUPERVISORY AUTHORITY

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

- 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 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 shall act as the 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: Commission nationale de l'informatique et des libertés (CNIL) - 3 Place de Fontenoy, 75007 Paris, France shall act as the competent supervisory authority.
- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority.
- Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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.

Data importer maintains a written security program for the security, integrity and protection of personal data it processes on behalf of its customers against unauthorized disclosure or loss. Data importer's security program includes administrative, technical and physical safeguards appropriate for data importer's size and resources and the types of information that it processes.

The following checklist sets out the description of the technical and organisational security measures implemented by the data importer in accordance with this annex:

- **Firewalls are used to protect our internet connections.**
- **The most appropriate secure settings for our devices and software are chosen and implemented.**
- **Access to your data and services is controlled.**
- **Ant-viruses and other anti-malware software and monitoring practices are deployed.**
- **Software and devices are kept up-to-date.**
- **Data is regularly backed-up.**

ANNEX III

LIST OF SUB-PROCESSORS

Identities of the Sub-processors used for the provision of the Services and their country of location are listed in the AVOXI privacy policy found at https://www.iubenda.com/privacy-policy/8179510/full-legal.

[1] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

Exhibit 2

UK GDPR International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: As set out in Annex I of Exhibit 1 Trading name (if different): As set out in Annex I of Exhibit 1 Main address (if a company registered address): As set out in Annex I of Exhibit 1 Official registration number (if any) (company number or	Full legal name: AVOXI, Inc. Trading name (if different): AVOXI Main address (if a company registered address): 300 Galleria Parkway, Suite 1040, Atlanta, Georgia 30339 Official registration number (if any) (company number or similar identifier): 0108647

	similar identifier): As set out in Annex I of Exhibit 1	
Key Contact	Full Name (optional): As set out in Annex I of Exhibit 1 Job Title: As set out in Annex I of Exhibit 1 Contact details including email: As set out in Annex I of Exhibit 1	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)	Data Exporter is deemed to have signed this Addendum by accepting AVOXI's Terms and Conditions or by entering into a Subscription Services Agreement with AVOXI	Data Importer is deemed to have signed this Addendum by accepting AVOXI's Terms and Conditions or by executing a Subscription Services Agreement with Data Exporter

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	✓ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: June 4, 2021 Reference (if any): The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 Other identifier (if any): N/A Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As set out in Annex I of Exhibit 1
Annex 1B: Description of Transfer: As set out in Annex I of Exhibit 1
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in Annex II of Exhibit 1
Annex III: List of Sub processors (Modules 2 and 3 only): As set out in Annex III of Exhibit 1

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ✓ Importer ✓ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "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";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.