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) ("**Service 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 and instructs the Data Processor to process personal data of individuals on its behalf.

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

Data Processing Agreement

This Data Processing Agreement ("**DPA**") is made on *[insert date*], between (i) Customer as defined in the CSA or SSA **(**"**Data Controller**"**)** and (ii) 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 a Service Agreement dated [*insert date*] in relation to the Data Processor providing telecommunications and call center software services to the Data Controller ("**Service Agreement**"). This DPA applies to the processing of personal data by the Data Processor in accordance with the scope of the Service Agreement that is subject to the Data Protection Laws (as defined in Clause 1.2 below). This DPA shall come into effect on the effective date of the Service Agreement and the term of this DPA shall correspond to the term of the Service Agreement. This DPA forms part of and is incorporated into the Service Agreement, and except as modified below, the terms of the Service 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 Service 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 Service 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 Service 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 Data Controller 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 Data Controller and in accordance with its documented instructions, for the sole purpose of performing its obligations under the Service Agreement or as otherwise reasonably instructed by the Data Controller, 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 Data Controller without undue delay.

2.3 At any time during the term of this DPA at the Data Controller's request or upon the termination or expiration of the Service Agreement, the Data Processor shall promptly return to the Data Controller 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 Data Controller 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 Data Controller 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 Data Controller, at the discretion of the Data Controller. 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 Data Controller's request. The Data Processor shall not materially decrease the overall security measures during the term of the Service Agreement.

4. Information and Audit

4.1 The Data Processor shall make available to the Data Controller on request all information necessary to demonstrate compliance with this DPA and the Data Protection Laws, and shall allow for audits, at Data Controller's sole expense, including on-site inspections, by the Data Controller or an auditor mandated by the Data Controller in relation to the Processing of the Personal Data. Data Controller 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 Data Controller's written request, the Data Processor shall make available to the Data Controller 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 Data Controller's expense and taking into account the nature of the Processing and the information available, provide the Data Controller with cooperation and assistance in relation to any data protection impact assessment or regulatory consultation that the Data Controller 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 Data Controller. The Data Controller'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 Data Controller'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 Data Controller 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 Data Controller of any new sub-processors the Data Processor intends to engage to process the Personal Data. The Data Controller 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 Data Controller 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 Data Controller, to respond to requests to exercise data subject rights under the Data Protection Laws.

6.2 The Data Processor shall promptly notify the Data Controller 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 Data Controller or as required by applicable laws to which the Data Processor is subject, in which case the Data Processor shall inform the Data Controller of that legal requirement before responding to the request. The Data Processor shall upon the Data Controller's request provide reasonable efforts to assist the Data Controller 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 Data Controller for damages suffered in relation to the Data Processor's breach of this DPA or Data Protection Laws, the Data Processor shall indemnify the Data Controller 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 Data Controller, 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 Service Agreement, it shall promptly notify the Data Controller about the incident, shall at all times cooperate with the Data Controller, and shall follow the Data Controller'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 Data Controller would violate applicable laws to which the Data Controller 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 Data Controller about an incident. Where the incident may require a data breach notification by the Data Controller 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 Data Controller 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 Data Controller'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 Data Controller 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 Data Controller;

(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 Service Agreement are reliable and trustworthy and have received the required training on the Data Protection Laws.

9. Indemnification

The Data Processor shall indemnify the Data Controller from and against all damages, including reasonable attorneys' fees, arising out of or resulting from any third party claims against the Data Controller 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.

This DPA is entered into and becomes a binding part of the Service Agreement with effect from the date first set out above between Customer and AVOXI.

Customer

____

AVOXI, Inc.

DocuSigned by:
Weston Edmunds
8DC6E5521C1D439...

____

Name: Weston Edmunds

Title: EVP

Schedule 1- Details of Processing

1. Personal Data

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

2. List of authorized sub-processors

The Data Controller 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 Data Controller

Email: That of Customer in the CSA or SSA

Address: That of Customer in the CSA or SSA

Contact information of the Data Processor.

Weston Edmunds, EVP
1000 Circle 75 Parkway, Suite 500, 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

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.

Disclaimer: This document was generated based on the text available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012 and is provided for convenience purposes. It should not be considered an authoritative text or legal guidance.

I. *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 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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(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.

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 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 ([2]) (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

(a) OPTION 2: 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 thirty days 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. ([3]) 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

(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. The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([4]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(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

(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

(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

(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 ([5]);

  (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. 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 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

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

OPTION 2: 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 Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(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 Republic of Ireland.

(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

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: That of Customer in the Services Agreement____

Address: That of Customer in the Services Agreement

Contact person's name, position and contact details: That of Customer in the Services Agreement

Activities relevant to the data transferred under these Clauses:

That to which Customer subscribed in the associated Services Agreement—either worldwide virtual telephone numbers or related telecommunications services or virtual contact center software

Signature and date: That of Customer in the associated Services Agreement

Role (controller/processor):

2. …

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

Address: 1000 Circle 75 Parkway, Suite 500, 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.

DocuSigned by:
Weston Edmunds
8DC6E5521C1D439...

Signature and date: ____

Role (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;
- IP address;
- Localization data;
- Device identification data

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 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:

- **We use firewalls to protect our internet connections.**
- **We choose the most appropriate secure settings for our devices and software.**
- **We control who has access to your data and services.**
- **We protect ourselves from viruses and other malware.**
- **We keep our software and devices up-to-date.**
- **We regularly backup our data.**

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] 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.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.