International Data Transfer Agreement

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The non-Acuity Scheduling, Inc. party to this Additional Agreement as defined in Acuity Scheduling Inc.'s Terms of Service Agreement to which these Standard Clauses are annexed

(the "data exporter")

And

Acuity Scheduling, Inc. ("Acuity")

Acuity Scheduling, % Registered Agents Inc.,
90 State Street, STE 700 Office 40
Albany, New York 12207

(the "data importer")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data

exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has

assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor

fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name of Customer: .....

Signature.....

Printed Name.....

Printed Title.....

Signature Date.....

On behalf of the data importer:

Gavin Zuchlinski, CEO

Signature.....

Acuity Scheduling, Inc.

Acuity Scheduling, % Registered Agents Inc.,
90 State Street, STE 700 Office 40
Albany, New York 12207

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Data exporter

The data exporter is the non-Acuity party to the Terms of Service Agreement (available at: https://acuityscheduling.com/tos.php) (the "Terms of Service" or the "Terms") to which these Standard Contractual Clauses are referred as an "Additional Agreement" thereto, as described in Section 1.5 of the Terms of Service. The data exporter is a user of Acuity's services as defined in the Terms of Service.

Data importer

The data importer is Acuity Scheduling, Inc., a Software as a Service company that provides calendaring and scheduling services to professional services providers and other businesses to help them schedule appointments, bookings, and meetings through a cloud service.

Data subjects

Data subjects include the data exporter's customer's representatives and end-users, primarily customers of the data exporter, but also including employees, contractors, and collaborators thereof. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by the data importer.

Categories of data

The personal data transferred includes, name, email and/or phone contact information, time and place of proposed appointment or booking, and other data in an electronic form in the context of Acuity's Services.

Processing Operations

The personal data transferred will be subject to the following basic processing activities.

a. **Duration and Object of Data Processing.** The duration of data processing shall be for the term designated under the Terms of Service between the data exporter and Acuity which is party to this Additional Agreement as defined in Section 1.5 of those Terms. The objective of the data processing is Acuity's performance of Services agreed to in those Terms.

b. **Scope and Purpose of Data Processing.** The scope and purpose of processing personal data is described in the Terms of Service. The data importer operates a network of data centers and management/support facilities, and processing may take place in any jurisdiction where Acuity or its sub-processors operate such facilities.

c. **Customer Data Access.** For the term designated under the Terms of Service Acuity will at its election, and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on its behalf.

d. **Data Exporter's Instructions.** In providing Services, Acuity will only act upon data exporter's instructions as conveyed by data exporter to Acuity in the course of data exporter's use of the Services.

e. **Customer Data Deletion or Return.** Upon expiration or termination of data exporter's use of Acuity's Services, it may extract Customer Data and data importer will delete Customer Data, each in accordance with the Product Use Rights applicable to the Agreement

Subcontractors

The data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain customer data only to deliver the services the data importer has retained them to provide, and they are prohibited from using customer data for any other purpose.

Effective Date: These Standard Contractual Clauses making up this Additional Agreement (including Appendices 1 and 2), are effective as of the effective date of this Additional Agreement.

On behalf of the data exporter:

Name of Customer: .....

Signature.....

Printed Name.....

Printed Title.....

Signature Date.....

On behalf of the data importer:

Gavin Zuchlinski, CEO

Acuity Scheduling, Inc.

Acuity Scheduling, % Registered Agents Inc.,
90 State Street, STE 700 Office 40
Albany, New York 12207

Signature.....

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. Personnel

Acuity's personnel will not process Customer Data without authorization. Personnel are obligated to maintain the confidentiality of any Customer Data and this obligation continues even after their engagement ends.

2. Data Privacy Contact

The data privacy officer of the data importer can be reached at the following address:

Acuity Scheduling Privacy Officer, % Registered Agents Inc.,

90 State Street, STE 700 Office 40

Albany, New York 12207

3. Technical and Organization Measures

a. General Practices. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data, as described in the Security Measures section of our Privacy Policy (available at: https://acuityscheduling.com/privacy.php) and also as described in this Additional Agreement and EU Standard Contractual Clauses, as against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

i. Organization of Information Security.

1. **Security Ownership.** Acuity has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.
2. **Security Roles and Responsibilities.** Acuity personnel with access to Customer Data are subject to confidentiality obligations.
3. **Risk Management Program.** Acuity performed a risk assessment before processing the Customer Data or launching the Services.
4. Acuity retains its security documents pursuant to its retention requirements after they are no longer in effect.

ii. Asset Management.

1. **Asset Inventory.** Acuity maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Acuity personnel authorized in writing to have such access.
2. **Asset Handling.**
   a. Acuity classifies Customer Data to help identify it and allow for access to it to be appropriately restricted (e.g. through encryption).
   b. Acuity imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data.
   c. Acuity personnel must obtain authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Acuity's facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing Customer Data from Acuity's facilities.

iii. Human Resources Security:

1. **Security Training.**

    a. Acuity informs its personnel about relevant security procedures and their respective roles. Acuity also informs its personnel of possible consequences of breaching the security rules and procedures.

iv. Physical and Environmental Security.

1. **Physical Access to Facilities**. Acuity limits access to facilities where information systems that process Customer Data are located to identified and authorized individuals.

2. **Physical Access to Components**. Acuity maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of Customer Data they contain.

3. **Protection from Disruptions.** Acuity uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

4. **Component Disposal.** Acuity uses industry standard processes to delete Customer Data when it is no longer needed.

v. Communications and Operations Management.

1. **Operational Policy.** Acuity maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

2. **Data Recovery Procedures.**

    a. On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Acuity maintains multiple copies of Customer Data from which Customer Data can be recovered.

    b. Acuity stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

    c. Acuity has specific procedures in place governing access to copies of Customer Data.

    d. Acuity reviews data recovery procedures at least every six months.

    e. Acuity logs data restoration efforts, including the person responsible, the description of the restored data and which data (if any) had to be input manually in the data recovery process.

3. **Malicious Software.** Acuity has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.

4. **Data Encryption.**

    a. Acuity encrypts Customer Data that is transmitted over public networks.

    b. Acuity restricts access to Customer Data in media leaving its facilities (e.g., through encryption).

5. **Event Logging**

    a. Acuity logs the use of our data-processing systems.

    b. Acuity logs access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

vi. **Access Control.**

1. **Access Policy.** Acuity maintains a record of security privileges of individuals having access to Customer Data.

2. **Access Authorization.**

   a. Acuity maintains and updates a record of personnel authorized to access Acuity systems that contain Customer Data.

   b. Acuity deactivates authentication credentials that have not been used for a period of time not to exceed six months.

   c. Acuity identifies those personnel who may grant, alter or cancel authorized access to data and resources.

   d. Acuity ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins.

3. **Least Privilege.**

   a. Technical support personnel are only permitted to have access to Customer Data when needed.

   b. Acuity restricts access to Customer Data to only those individuals who require such access to perform their job function.

4. **Integrity and Confidentiality.**

   a. Acuity instructs its personnel to disable administrative sessions when leaving premises Acuity controls or when computers are otherwise left unattended.

   b. Acuity stores passwords in a way that makes them unintelligible while they are in force.

5. **Authentication.**

   a. Acuity uses industry standard practices to identify and authenticate users who attempt to access information systems.

   b. Where authentication mechanisms are based on passwords, Acuity requires that the passwords are renewed regularly.

   c. Where authentication mechanisms are based on passwords, Acuity requires the password to be at least six characters long.

   d. Acuity ensures that de-activated or expired identifiers are not granted to other individuals.

   e. Acuity monitors repeated attempts to gain access to the information system using an invalid password.

   f. Acuity maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

   g. Acuity uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

6. **Network Design.**

   a. Acuity has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.

vii. **Information Security Incident Management.**

1. **Incident Response Process.**

a. Acuity maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

b. Acuity tracks disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.

c. **Service Monitoring.** Acuity security personnel verify logs at least every six months to propose remediation efforts if necessary.

viii. Business Continuity Management.

1. Acuity maintains emergency and contingency plans for the facilities in which Acuity information systems that process Customer Data are located.

2. Acuity's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original state from before the time it was lost or destroyed.

ix. The security measures described in this Section set forth Acuity's responsibility with respect to the security of Customer Data and do not contemplate or require additional or increased security measures.

On behalf of the data exporter:

Name of Customer: .....

Signature.....

Printed Name.....

Printed Title.....

Signature Date.....

On behalf of the data importer:

Gavin Zuchlinski, CEO

Signature.....

Acuity Scheduling, Inc.

Acuity Scheduling, % Registered Agents Inc.,
90 State Street, STE 700 Office 40
Albany, New York 12207