DATA PROCESSING ADDENDUM

This Data Processing Addendum ("***DPA/Addendum***") establishes minimum data protection and cyber security standards and related requirements for Scitara Corporation and/or its Affiliate(s) ("***Processor***" or "***Scitara***") in connection with its performance of services for Customer ("***Controller***" or "***Customer***") (each a "***Party***" and collectively the "***Parties***").

This Data Processing Addendum supplements the Master Services Agreement ("***Master Agreement/Agreement***") entered into by and between the Customer and Scitara Corporation which describes the services provided by Scitara ("***Scitara System***" or "***Services***"). This DPA is hereby incorporated into the Master Agreement between the parties. Controller enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws (*defined below*), in the name and on behalf of its Affiliates (*defined in the Master Agreement*), if any. This DPA incorporates the terms of the Agreement, and any terms not defined in this DPA shall have the meaning set forth in the Master Agreement. In the event of a conflict between the terms and conditions of this DPA and the Master Agreement, the terms and conditions of this DPA shall supersede and control.

In consideration of the mutual covenants and promises herein, the Parties intending to be legally bound, hereby agree as follows:

1. **Definitions**.

(A) "***Covered Information***" means, in any form, format or media, any (a) confidential information of Customer under the Master Agreement; and/or (b) Personal Data.

(B) "***Data Security Breach***" means, in connection with the Services, (i) the loss or misuse (by any means) of Covered Information; (ii) the inadvertent, unauthorized, and/or unlawful disclosure, access, alteration, corruption, transfer, sale, rental, destruction, or use of Covered Information; or (iii) any other act or omission that compromises or may compromise the security, confidentiality, or integrity of Covered Information or a System.

(C) "***Personal Data***" means any and all information provided by Customer to Scitara or otherwise Processed by Scitara on behalf of Customer and/or its Affiliates (i) that identifies, either alone or in combination with other information, an individual, or (ii) from which identification or contact information of an individual person can be derived.

(D) "***Process***" (including its cognates, "Processing" and "Processed") means any operation or set of operations that is performed upon Personal Data or Covered Information, whether or not by automatic means, including, but not limited to, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deletion, erasure, or destruction.

(E) "***Services***" means those services, including without limitation Processing, that Scitara performs pursuant to the Master Agreement.

(F) "***Sub-Processor***" means a person or entity engaged by Scitara to assist it in fulfilling its obligations under the Agreement.

(G) "***System***" means any system, network, platform, database, computer, or telecommunications or other information system owned, controlled or operated by or on behalf of Customer or any of its Affiliates.

(H) "***Insufficient Security***" means any lapse, error in, gap, or lack of data security protection that results in, or can reasonably be expected to result in, a Data Security Breach of Covered Information or a System.

2. **General Requirements**.

(A) **Controller** may, at its sole discretion, provide or make accessible to Processor Covered Information to Process on behalf of Controller. Controller represents and warrants that:

i) Controller shall ensure the accuracy, quality, and legality of (1) Personal Data provided to Processor by or on behalf of Controller; (2) means by which Controller acquired any such Personal Data; and (3) instructions it provides to Processor regarding the Processing of such Personal Data.

ii) Controller's instructions to the Processor shall comply with all laws, rules and regulations applicable in relation to the Personal Data;

iii) Processing of Personal Data in accordance with Controller's instructions shall not cause Processor to be in breach of the Data Protection Laws.

iv) Controller shall not provide or make available to Processor any Personal Data in violation of the Master Agreement or otherwise inappropriate for the nature of the Services and shall indemnify Processor from all claims and losses in connection therewith.

(B) **Processor** represents and warrants that:

i) Processor shall Process Covered Information only on behalf of Controller and solely to the extent necessary to provide the Services to Controller and in accordance with applicable laws and the written instructions of Controller, as applicable, as issued by Controller from time to time;

ii) Processor has implemented adequate technical and organizational security measures with respect to Covered Information, including at least those measures set forth in Section 4 of this Agreement;

iii) Processor ensures that personnel with access to Covered Information are subject to a contractual or statutory duty of confidentiality;

iv) Processor shall promptly notify Controller about:

(1) any Data Security Breach in accordance with Section 4(D) of this Agreement; and

(2) any request, inquiry, complaint, notice or communication received from any third party, including a data subject or a supervisory authority, with respect to any Personal Data and will comply with instructions of Controller in providing assistance to respond to such request, inquiry, complaint, notice or communication, provided that Controller is itself unable to respond without Processor's assistance;

(3) any instruction by Controller that Processor believes to be in violation with applicable laws;

v) Processor shall not disclose Covered Information to third parties (including Sub-Processors) unless such disclosure is:

(1) necessary to perform the Services and provided that Processor (i) has received the prior written approval of Controller to use the services of such Sub-Processor; (ii) enters into a written, valid and enforceable agreement with such Sub-Processor that includes terms that are no less restrictive than the obligations applicable to Processor under the this Agreement; (iii) conducts initial and periodic assessments of the privacy and security safeguards and practices of the Sub-Processor to ensure that such Sub-Processor complies with such obligations; and (iv) remains responsible for any breach of the obligations set forth in this Agreement; or

(2) required by applicable laws or compulsory legal process, in which case Processor shall to the extent legally permissible, notify Controller promptly in writing before complying with any such disclosure request, and shall comply with all reasonable directions of Controller with respect to such disclosure;

vi) At Controller's request, Processor shall, no more than once per calendar year, either (i) make available for Controller's review copies of certifications or reports demonstrating Processor's compliance with its obligations under this Data Processing Agreement, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Controller or its authorized representative reasonably acceptable to Processor, upon thirty (30) days' prior written notice and at a mutually agreeable date and time, to conduct an audit to demonstrate Processor's compliance with its obligations under this Data Processing Agreement. Controller shall provide thirty (30) days' prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Processor's business. Controller shall be responsible for the costs of any such audits, including without limitation a reimbursement to Processor for any time expended for on-site audits.

vii) Processor shall not transfer any Personal Data from any jurisdiction to any other jurisdiction without Controller's prior written consent and, if applicable, without putting in place an appropriate transfer agreement or other mechanism appropriate to comply with applicable data protection laws, and, to the extent that Processor receives Personal Data from any jurisdiction in reliance on a government approved data transfer framework. Processor further represents and warrants that it shall comply with such framework during the term of the Master Agreement and during such time as Processor Processes Personal Data;

viii) If Processor is located in the EU and transfers any Personal Data to an affiliate, subcontractor or other entity located outside the EU ("non-EU entity"), Processor and such non-EU entity shall enter into the Standard Contractual clauses or shall otherwise comply with Chapter V of the General Data Protection Regulation 2016/679 ("GDPR"). If Processor is located outside the EU, the Standard Contractual clauses as contained hereinbelow are incorporated herein by reference and become a part of this DPA mutually enforceable by the parties.

ix) Processor shall enter into additional agreements with Controller governing the Processing of Personal Data where reasonable or required by applicable data protection laws;

x) Processor shall duly assist and cooperate with Controller to allow Controller to comply with its obligations under applicable data protection laws, including, but not limited to, the rights of data subjects, requests and notices served by supervisory authorities on Controller in relation to the Processing of Personal Data pursuant to the Master Agreement and the conduct of privacy impact assessments to assess the privacy risks attendant upon a particular data processing activity; and

xi) Processor shall retain Covered Information only for as long as necessary to perform the Services, or as required by applicable laws, and in all cases the terms of this Agreement continue to apply with respect to such Personal Data during all periods in which it is retained by Processor, including for any period after expiration or termination of the Agreement.

3. <u>Authorized Sub-Processors.</u>

(A) Controller acknowledges and agrees that Processor may (1) engage its affiliates and the Authorized Sub-Processors to Process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the Processing of Personal Data. By way of this DPA, Controller provides general written authorization to Processor to engage sub-processors as necessary to perform the Services.

(B) A list of Processor's current Authorized Sub-Processors (the "List") will be made available to Controller, and may be updated by Processor from time to time. At least ten (10) business days before enabling any third party other than Authorized Sub-Processors to access or participate in the Processing of Personal Data, Processor will add such third party to the List. Controller may reasonably object to such an engagement on legitimate grounds by informing Processor in writing within ten (10) business days of receipt of the aforementioned notice by Controller. Controller acknowledges that certain sub-processors are essential to providing the Services, or an aspect of the Services, and that objecting to the use of a sub-processor may prevent Processor from offering the Services, or an aspect of the Services, to Controller.

(C) If Controller reasonably objects to an engagement in accordance with Clause 3(B), and Processor cannot provide a commercially reasonable alternative within a reasonable period of time, Controller may terminate this DPA. Termination shall not relieve Controller of any fees owed to Processor under the Agreement.

(D) If Controller does not object to the engagement of a third party in accordance with Clause 3(B) within ten (10) business days of notice by Processor, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.

(E) Processor will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Processor under this DPA with respect to the protection of Personal Data. Processor will remain liable to Controller for the performance of the Authorized Sub-Processor's obligations under such agreement.

(F) If Controller and Processor have entered into Standard Contractual Clauses, the above authorizations in Clause 3 will constitute Controller's prior written consent to the subcontracting by Processor of the processing of Personal Data if such consent is required under the Standard Contractual Clauses.

4. **<u>Cyber and Information Security</u>**.

(A) Without limitation to its other obligations under the Agreement, Processor represents and warrants that:

i) Processor shall comply with all applicable laws and privacy standards, and shall establish and maintain administrative, technical, and physical safeguards designed to ensure the security, confidentiality, reliability and integrity of Covered Information, as well as any Systems, facilities, or software that Processor accesses or supports in connection with the services being provided to Controller. Such safeguards would be commensurate with the type and amount of Covered Information Processed by Processor, having regard to the state of the art and industry standards, and would be aimed, at a minimum, to protect Covered Information and Systems against reasonably anticipated threats or hazards, including from unauthorized access, loss, theft, destruction, use, modification, collection, attack, or disclosure.

ii) Processor shall establish, maintain and comply with a written security program and policy that meets or exceeds the requirements imposed under applicable laws and aligns with industry best practices.

(B) Processor shall ensure that all its employees, Sub-Processors and agents are advised of and comply with, and are appropriately trained regarding, (i) Data Protection and information security training; and (ii) the provisions of this Agreement regarding the confidentiality, privacy and security of Covered Information.

(C) Processor shall provide to Controller, without undue delay, written notice of any suspected or confirmed Data Security Breach affecting Covered Information after becoming aware of such suspected or confirmed Data Security Breach. Such notice shall summarize such details concerning the Data Security Breach as Controller may reasonably request (including details regarding Covered Information that was or may have been compromised).

(D) In the event of any suspected or confirmed Data Security Breach, Processor shall taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance necessary for Controller to comply with its obligations under the applicable laws with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay. Processor's obligation to report or respond to a Personal Data Breach will not be construed as an acknowledgement by Processor of any fault or liability with respect to the Personal Data Breach.

5. **Confidential Information**.

Processor expressly confirms and acknowledges that any confidential information related to Controller that is Processed by Processor may include Personal Data in which case any and all of the confidentiality obligations shall apply to such information.

6. **Termination**.

Upon termination of the applicable Sales Order(s), or at any time upon Company's request, Scitara shall immediately return all Personal Data to Customer or shall destroy all Personal Data and certify to Customer that it has done so, unless Scitara is required by applicable laws to retain such data or a part thereof. Customer to be notified in writing in the event that Scitara is required by law to retain full or partial data.

7. **Limitation of Liability**.

The total liability of each of Controller and Processor (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Master Agreement.

8. **Miscellaneous**.

To the extent not inconsistent herewith, the applicable provisions of other arrangements (including without limitation choice of law, confidentiality, termination, enforcement, and interpretation) shall apply to this Agreement. The obligations in this Agreement shall never expire to the extent that Personal Data continues to be Processed by Processor on behalf of Controller. This Agreement may be executed in counterparts, each of which shall be deemed an original, and all such counterparts together shall constitute but one and the same instrument.

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) 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 the 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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 authorized 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 (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 defense 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) SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorization. The data importer shall submit the request for specific authorization at least [10] ten business days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide

on the authorization. The list of sub-processors already authorized by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(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. 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 authorized 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 organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

(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;

(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

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of EU Member State within whose jurisdiction the Controller is established.]

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 the EU Member State within whose jurisdiction the Controller is established.

(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

ANNEX I

A. LIST OF PARTIES

***Data exporter(s)*:**

Name: The Organisation or Entity identified as "Customer" in the Sales Order(s)

Address: The address for Customer as specified in the Sales Order(s)

Contact person's name, position and contact details: The contact details associated with the Customer as specified in the Sales Order(s)

Activities relevant to the data transferred under these Clauses: The activities as specified in the Sales Order(s)

Signature and date: By agreeing to the terms of the Master Service Agreement and the Sales Order(s), the data exporter will be deemed to have signed this Annex I.

Role (controller/processor): **Controller**

***Data importer(s)*:**

Name: Scitara Corporation

Address: 11 Apex Drive, Suite 300A, Marlborough, MA 01752

Contact person's name, position and contact details: The contact details for Scitara as mentioned in the Sales Order(s)

Activities relevant to the data transferred under these Clauses: The activities as specified in the Sales Order(s)

Signature and date: By agreeing to the terms of the Sales Order(s), the data importer will be deemed to have signed this Annex I.

Role (controller/processor): **Processor**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred. The data subjects could include the authorized users of the customer.

Categories of personal data transferred. The personal data provided by the Customer to Scitara.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. The data exporter may not include sensitive personal data in the personal data.

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

Nature of the processing. Compute, storage, provide access to service and other services as described in the Sales Order(s).

Purpose(s) of the data transfer and further processing. To provide the service and technical support.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period. The period for which the personal data will be retained will be in accordance with the terms of the Addendum.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing. The subject matter, nature and duration of processing in case of transfer to sub-processors will be as specified in the Addendum and the Sales Order(s).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13. The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

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

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

The technical and organizational measures as well as the scope and extent of assistance required to respond to the data subjects' requests are described in the Master Services Agreement and the Addendum.

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

The technical and organizational measures that the data importer will impose on the sub-processors are described in the Master Services Agreement and the Addendum.

ANNEX III

LIST OF SUB-PROCESSORS

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

1. ***Name***: Amazon Web Services
   Address: Amazon Web Services, Inc., PO BOX 84023, Seattle, WA 98124-8423, US
   Contact person's name, position and contact details: The sub-processor may be contacted through https://aws.amazon.com/contact-us/compliance-support/ or through Scitara contact provided in the Sales Order(s).
   Description of processing *(including a clear delimitation of responsibilities in case several sub-processors are authorized)*: Cloud computing services.

2. ***Name***: MongoDB
   Address: 1633 Broadway, 38th floor, New York, NY 10019
   +1 (866) 237-8815
   Contact person's name, position and contact details: The sub-processor may be contacted at privacy@mongodb.com or through Scitara contact provided in the Sales Order(s).
   Description of processing *(including a clear delimitation of responsibilities in case several sub-processors are authorized)*: Database management system.

3. ***Name***: Zendesk
   Address: 989 Market St. San Francisco, CA 94103
   +1(888) 670-4887
   Contact person's name, position and contact details: The sub-processor may be contacted at privacy@zendesk.com or through Scitara contact provided in the Sales Order(s).
   Description of processing *(including a clear delimitation of responsibilities in case several sub-processors are authorized)*: Incident and issue management system; sharing FAQs and knowledge-based articles.