DATA PROCESSING ADDENDUM

These Data Processing obligations set for the Client's data privacy and data protection obligations. All capitalized terms not otherwise defined herein will have the same meaning as ascribed to them in the Agreement.

1. DEFINITIONS

1.1 "Agreement" shall mean all agreements between Omeda and Client relating to the provision of services by Omeda and/or its Affiliates to Client.

1.2 "Affiliate" means any entity controlling, controlled by, or under common control with a party.

1.3 "Client Personal Data" means the Personal Data of Data Subjects whose data Omeda is Processing as Processor on behalf of Client in order to provide the Services.

1.4 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

1.5 "Data Protection Law(s)" means any law in any region, including the United States, United Kingdom ("UK"), where applicable, the GDPR, or Swiss data protection law and regulations or rules applicable to preservation of personal privacy rights and the protection Client Personal Data.

1.6 "EEA" means the European Economic Area.

1.7 "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

1.8 "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2. ROLE AND SCOPE OF PROCESSING

2.1 With regard to the Processing of Client Personal Data under this Addendum, Client is the Controller and Omeda is the Processor and Service Provider.

2.2 Omeda will Process the Client Personal Data only for the purpose of providing the Services to Client under the Agreement and in accordance with Client's documented instructions. Omeda shall promptly notify Client if Omeda believes that any instruction given by Client regarding Processing violates any Data Protection Law.

2.3 Client and Omeda hereby acknowledge and agree that in no event shall the transfer of Personal Data from Client to Omeda as a Service Provider pursuant to the Agreement constitute a sale of data or transfer of data for valuable consideration, and that Omeda is granted a limited license to access Personal Data as required for performance under this Agreement.

3. SUB-PROCESSING

3.1 Client hereby agrees that Omeda may retain as Sub-processors: (i) Omeda's Affiliates; and (ii) third parties engaged by Omeda and Omeda's Affiliates. The list of current third-party Sub-processors is found [HERE]

3.2 Omeda shall be liable for the acts and omissions of its Sub-processors to the same extent Omeda would be liable if performing the Services of each Sub-processor directly under the terms of this Addendum.

4. RIGHTS OF DATA SUBJECTS

4.1 To the extent permitted by law, and to the extent such request is reasonably identifiable as relating to the Services provided to Client, Omeda will notify Client of requests from Data Subjects exercising their Data Subject Access Rights.

4.2 Client shall pay any Charges relating to Omeda's provision of the foregoing assistance, including where assistance is provided outside the existing scope of the Services.

5. COOPERATION

To the extent Omeda is required under Data Protection Laws, Omeda will assist Client to conduct a data protection impact assessment and, where legally required, consult with applicable regulatory or supervisory authorities in respect of any proposed Processing activity that present a high risk to Data Subjects.

6. DATA ACCESS & SECURITY

Omeda shall ensure that its personnel engaged in the Processing of Client Personal Data have been informed of the confidentiality of the Client Personal Data or are under an appropriate contractual obligation of confidentiality. Omeda shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk in Processing the Client Personal Data in the provision of the Services. Omeda will notify Client without undue delay upon becoming aware of a Personal Data Breach with respect to the Client Personal Data, unless it is prohibited to do so by law enforcement.

7. INTERNATIONAL TRANSFERS

7.1 Omeda's use of Client Personal Data as permitted under the Agreement shall include transfers of Personal Data (including in connection with the provision of Services or in response to Client's direction or request) outside the EEA, the UK, and/or Switzerland, and Omeda and its Affiliates may Process the Client Personal Data in the United States of America and any other jurisdictions in which Omeda, its Affiliates, and their respective Sub-processors are located.

7.2 By agreeing to this Addendum, Client is entering into the Model Clauses found [HERE].

8. RETENTION, RETURN, AND DELETION OF CLIENT PERSONAL DATA

8.1 Subject to Data Protection Law, if any Data Subject undergoes a period of six (6) years of Inactivity during the term of the Agreement, Client instructs Omeda to delete or destroy the Client Personal Data corresponding to such Data Subject so as to render it forensically irretrievable.

8.2 Omeda shall destroy or return to Client all Client Personal Data retained by Omeda, and Client shall reimburse Omeda for any Charges relating to the return or destruction of the Client Personal Data.

9. CLIENT OBLIGATIONS

Client shall comply with Data Protection Laws and carry out each of the responsibilities of a Controller under the GDPR and any other Data Protection Laws. Client represents, warrants, and covenants that Client either has met, or will meet, prior to provision of any Client Personal Data to Omeda, all requirements of law (including, without limitation, the GDPR and other Data Protection Laws, and Client's specific obligations to obtain explicit consent to process any 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 data or as otherwise may be deemed sensitive under Data Protection Laws) applicable to the provision of Client Personal Data to Omeda to enable Omeda to lawfully Process such Client Personal Data consistent with Omeda's rights and obligations under the Agreement and this Addendum.

Client shall maintain Cyber Liability Policy Insurance with minimum limits of Five Million Dollars ($5,000,000.00) per occurrence, including, without limitation, coverage for computer networks security breaches, implementation of a malicious code or malware, theft or destruction of data, and unauthorized access to devices, computers, computer systems or networks.

10. LIABILITY

Notwithstanding any exclusions of liability or limitations of liability under the Agreement, Client shall fully indemnify Omeda, its Affiliates, and its and their respective officers, directors, shareholders, employees, contractors, agents, successors, and assigns against all liabilities, costs, expenses, damages, and losses (including but not limited to any direct, indirect, or consequential losses, loss of profit, loss of reputation and all fines, interest, penalties, and legal costs, including reasonable attorneys' fees) suffered or incurred by Omeda arising out of: (i) Processing the Client Personal Data in accordance with Client's documented instructions; or (ii) Client's breach of Section 10 hereof.

11. UPDATES TO ADDENDUM

Omeda may change the terms of this Addendum if the change (i) is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency.

12. GENERAL

For clarity, if Client has entered into more than one Agreement, this Addendum will amend each of the Agreements separately. This Addendum shall be coterminous with the Agreement.

SCHEDULE 1

EUROPEAN COMMISSION

DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship

Unit C.3: Data protection

Commission Implementing Decision (EU) 2021/914
Standard Contractual Clauses (processors)

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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) (1), and in particular Article 28(7) and Article 46(2)(c) thereof, Name of the data exporting organisation: The Client listed in Section 1 of the Data Processing Addendum Cover Page

(the data **exporter**)

And

Name of the data importing organisation: Those entities listed in Annex I. and which are signatories to these Clauses.

(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 Annex I.

Clause 1

Purpose and scope

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

[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

(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) Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Modules Two 12(a), (d) and (f);
(iv) Clause 13;
(v) Clause 15.1(c), (d) and (e);
(vi) Clause 16(e);
(vii) Clause 18 – Modules Two: Clause 18(a) and (b).

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. (1)

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 **Instructions**

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

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

8.2 **Purpose limitation**

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

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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 noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

[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. (4)

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least annually 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

MODULE TWO: Transfer controller to processor

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

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

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. (8)

(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 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.

MODULE TWO: Transfer controller to processor

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

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

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

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

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

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

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

Clause 12

Liability

MODULE TWO: Transfer controller to processor

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

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

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

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

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

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

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

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

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

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(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.

[4] 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. (12)

(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

MODULE TWO: Transfer controller to processor

15.1 **Notification**

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

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

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

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

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

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

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

15.2 **Review of legality and data minimisation**

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

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

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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

(b) The Parties agree that those shall be the courts of Germany.

(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 1 to the Standard Contractual Clauses

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is the Client listed in Section 1 of the Data Processing Addendum Cover Page.

Data importer
The data importer is those entities listed in Appendix 3 and which are signatories to these Clauses.

Data subjects
The personal data transferred concern the categories of data subjects listed in Section 2 of the Data Processing Addendum Cover Page.

Categories of data
The personal data transferred concern the categories of data listed in Section 2 of the Data Processing Addendum Cover Page.

Special categories of data (if appropriate)
The personal data transferred does not concern special categories of data.

Processing operations
The personal data transferred will be subject to the processing basic activities listed in Section 2 of the Data Processing Addendum Cover Page.

Annex I.B. to the Standard Contractual Clauses

1. **Nature and Purpose of the Processing.** Omeda's Processing of Client Personal Data in relation to its provision of the following Services to Client, as further described in the parties' Agreement, including:
   - ✓ Print Fulfillment
   - ✓ Email Deployments
   - ✓ Digital Editions Distribution
   - ✓ Subscriber Marketing
   - ✓ Subscription Permission Management
   - ✓ Data Management
   - ✓ Website Analytics
   - ✓ Content Personalization
2. **Duration of the Processing.** The period from the Effective Date through the expiration of the term of the Agreement, plus the period of time from the expiration of the term of the Agreement until all Client Personal Data has been returned to Client or destroyed.
3. **Categories of Personal Data**:
   - ✓ Contact Information (e.g., first name, last name, email, phone number)
   - ✓ Postal Mailing Address
   - ✓ Business Card Information (e.g., title, company)
   - ✓ Business Demographic Information (e.g., company size, industry)
   - ✓ Non-Special Category Demographic Information (e.g., age)
   - ✓ Website User Activity Data
   - ✓ Content Consumption Information
   - ✓ Event Attendance Information
   - ✓ Email Recipient Activity Information
   - ✓ Product Subscription Information
   - ✓ Financial and Payment Information
   - □ OTHER (please describe): ____
4. **Categories of Data Subjects**:
   - ✓ Client's employees, contact persons, agents, advisors, freelancers (who are natural persons)
   - ✓ Client's customers, prospective customers, business partners and vendors (who are natural persons)
   - ✓ Employees or contact persons of Client's customers, prospective customers, business partners and vendors
   - ✓ Client's users authorized by Client to use the Services provided by Omeda

Annex I.C. to the Standard Contractual Clauses

Supervisory Authority:

Germany - State Data Protection Commissioners

Germany - Conference of Independent German Federal and State Data Protection Supervisory Authorities (DSK)

Germany - Federal Commissioner for Data Protection and Freedom of Information

Annex II to the Standard Contractual Clauses

This Annex II forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 8.3 and 8.6 (or document/legislation attached):

As of the Effective Date, Omeda will implement and maintain the security measures set out in this Annex II. Omeda may update or modify such security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services.

Omeda, itself or through its vendors and/or Sub-processors, implements and maintains the following technical and organizational security measures:

Physical Security

Data Center

Infrastructure. Omeda stores all production systems and data on servers located at a secure colocation data center operated by a third-party vendor ("Service Provider"). The colocation facility features an Operations Service Center that manages all aspects of the facility, while upholding the utmost in customer satisfaction as measured by an industry-leading Net Promoter Score that exceeds similar B2B technology organizations. The Service Provider employs in-house security, facility maintenance and audit teams that meet multi-industry compliance standards using automated systems.

Redundancy. Infrastructure systems are designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks and other necessary devices help provide this redundancy. This infrastructure allows Omeda to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented procedures that detail the process and frequency of preventative maintenance and performance standards in accordance with either the manufacturer's specifications or internal requirements. Preventative and corrective maintenance of the data center equipment is scheduled through a standard process according to documented procedures.

Power. Power systems at the colocation facility operated by the Service Provider are designed to be redundant and maintainable without disruption to ongoing operations. Dual utilities are combined with a third emergency utility line and segregated electrical and mechanical rooms to supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power via UPS is designed to provide transitory power to the data center, at full capacity, until the emergency systems powered by industrial generators take over. The generators are designed to automatically start up within seconds to provide sufficient emergency electrical power to run the data center at full capacity for several days.

Server Hardware. Omeda servers use hardened operating systems which are customized in accordance with business requirements. Data storage methods (RAID, replication, etc.) are similarly customized to provide additional security and redundancy.

Business Continuity. Omeda backs up and replicates data over multiple systems located on servers at the co-location and in the cloud to protect against accidental destruction or loss of client data.

Physical Site Controls

Data Center Security Operation. The Service Provider’s colocation data center is secured by perimeter fencing, a single point of entrance, 2-factor biometric authentication (fingerprint and iris scan), on-site security, and closed-circuit video cameras covering the interior and exterior of the building.

Data Center Access Procedures and Security Devices. The Service Provider maintains security procedures and systems restricting physical access to the colocation data center by unauthorized personnel. In addition to exterior fencing, security cameras and regular patrols, electronic card key access is provided only to authorized employees, contractors and visitors. Data center electronic card key access requests must be made in advance and in writing, and require the approval of the requestor's manager and the Service Provider’s director. All other entrants requiring temporary access to the data center must: (i) obtain approval in advance from the data center manager for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

In addition to an electronic card key system, the Service Provider employs a biometric (retina and fingerprint) access control system that is linked to an alarm system. The access control system monitors and records each visitor's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated by the Service Provider’s security personnel. Authorized access throughout the business operations and data center is restricted based on zones and the individual's job responsibilities. The fire doors at the data center are alarmed. CCTV cameras are in operation throughout the facility both inside and outside the data center. The positioning of the cameras has been designed to cover strategic areas including, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment.

Digital Security

Access Control

Infrastructure Security Personnel. Omeda maintains a data security policy for its personnel, and requires security training for employees. Omeda's infrastructure security personnel are responsible for the ongoing monitoring of Omeda's infrastructure, review of the services provided by Omeda, and responding to security incidents.

Access Control and Privilege Management. Clients, administrators and users must authenticate themselves via a central authentication system or via a single sign-on system in order to use the services provided by Omeda.

Internal Data Access Processes and Policies. Omeda's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Omeda aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing. Omeda employs a centralized access management system to control access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing SSH certificates are designed to provide Omeda with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Omeda requires the use of unique user IDs, strong passwords to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and on a need-to-know basis. The granting or modification of access rights must also be in accordance with Omeda's internal data access policies. Access to systems are logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and use of strong passwords.

Networks & Data Transmission

Data Transmission. Omeda’s offices are connected to its equipment at the Service Provider’s colocation data center via high-speed private links. The private links provide secure and fast data transfer between connected systems. These links are designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Omeda transfers data via standard Internet protocols.

Encryption In-Transit & At-Rest. Omeda utilizes secure protocols (HTTPS, SSH, IPSEC, etc.) to encrypt and protect sensitive data in transit. Data at rest (such as the physical and virtualized hard drives used by Omeda database server instances, and long-term storage solutions like AWS) is protected by AES-256 encryption.

Intrusion Detection/Prevention. Omeda employs multiple layers of network devices and intrusion detection technologies to help protect its external attack surface. Potential attack vectors are analyzed, and appropriate purpose-built technologies are incorporated into public-facing systems. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Omeda's intrusion detection involves:

1. Limiting the potential attack surface through preventative measures;
2. Incorporating detection controls at data entry points; and
3. Employing technologies to automatically remedy high-risk situations.

Incident Response. Omeda monitors a variety of communication channels for security incidents, and Omeda's Incident Response Team will react promptly to known incidents.

Data Storage, Isolation & Authentication

Omeda stores data in a multi-tenant environment. Omeda logically isolates each customer's data. A central authentication system is used across disparate systems and services to increase uniform security of data.

Decommissioned Disks and Disk Destruction Guidelines

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned. These decommissioned disks are subject to a series of data destruction processes (per Omeda processes and policies). If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be physically destroyed.

Personnel & Sub-processor Security

Personnel Security

Omeda personnel are required to adhere to the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. In accordance with applicable local labor law and statutory regulations, appropriate background checks are conducted for Omeda personnel, and personnel are required to execute a confidentiality agreement. Further, they must acknowledge receipt of, and compliance with, Omeda's confidentiality and privacy policies. Omeda's personnel will not process personal data without authorization, and personnel handling personal data are required to complete additional requirements relevant to their role.

Sub-processor Security

Omeda conducts an audit of the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Omeda has assessed the risks presented by the Sub-processor, the Sub-processor is required to enter into appropriate security, confidentiality and privacy contract terms.