Data Processing Addendum

Published on: 13 October 2022

Usage Note: This Data Processing Addendum is applicable if Azeus processes any personal data on the Customer's behalf when performing its obligations under the Agreement (as defined below), and that the Customer or its End Users are subject to applicable data protection laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom such as the EU General Data Protection Regulation.

For questions, please contact dataprocessing@azeus.com .

This Data Processing Addendum ("**DPA**") forms a part of the Convene ESG Licenses and Services Purchase Agreement, Convene ESG Terms of Service (at https://www.conveneesg.com/terms/), or other written or electronic agreement between Azeus and Customer for the use or subscription of Convene ESG services from Azeus, unless Customer has entered into a superseding written purchase or subscription agreement with Azeus, in which case, it forms a part of such written agreement (in either case, the "**Agreement**"). This DPA shall vary any existing data protection provisions that apply to the processing of Customer Personal Data in the manner and to the extent specified in this DPA.

By registering for an account or using any of the Services, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of other Controller(s) including its Controller Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Controller Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services under the Agreement, Azeus may Process certain Personal Data (such terms defined below) on behalf of Customer, and where Azeus Processes such Personal Data on behalf of Customer, the parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

IF YOU DO NOT AGREE WITH THIS DPA, OR DO NOT HAVE THE AUTHORITY TO AGREE TO THIS DPA ON BEHALF OF YOUR **COMPANY, CORPORATION, PARTNERSHIP, ASSOCIATION, GOVERNMENT, GOVERNMENT INSTITUTION, GOVERNMENT OWNED AND CONTROLLED CORPORATION, PUBLIC OR PRIVATE EMPLOYER, PRINCIPAL, OR ANY OTHER ENTITY OR PERSON FOR WHICH/WHOM YOU PURPORT TO BE AN AGENT, EMPLOYEE OR REPRESENTATIVE (COLLECTIVELY REFERRED HEREAFTER AS "ORGANIZATION"),**YOU MUST NOT REGISTER FOR AN ACCOUNT WITH US AND MUST NOT USE THE SERVICES.

HOW THIS DPA APPLIES TO CUSTOMER AND ITS AFFILIATES:

If the Customer entity entering into this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.

If the Customer entity entering into this DPA has executed an Order Form with Azeus pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms.

If the Customer entity entering into this DPA is neither a party to an Order Form nor an Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

1. DEFINITIONS

"Azeus" means the Azeus entity that entered into the Agreement.

"Azeus Group" means Azeus and its Affiliates.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Controller Affiliate**" means any of Customer's Affiliate(s) (a) (i) that are subject to applicable Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (ii) permitted to use the Services pursuant to the Agreement between Customer and Azeus, but have not signed their own Order Form and are not a "Customer" as defined under the Agreement, (b) if and to the extent Azeus processes Personal Data for which such Affiliate(s) qualify as the Controller.

"Customer" means the company or organization that entered into the Agreement with Azeus.

"Customer Data" means Content or other information (such as emails, messages or data) submitted by Customer or End Users to the Services or to Azeus in relation to the Agreement (such as seeking helpdesk or technical support).

"Data Protection Laws" means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"EU GDPR" means the 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).

"International Data Transfer Agreement" refers to an appropriate safeguard that can be used by organisations to make transfers of personal data from the United Kingdom to countries overseas and to be used by parties which ensures that the relevant protections for data subjects of the transferred data are sufficiently similar to those offered under UK data protection law, issued under Section 119A of the Data Protection Act 2018 and following Parliamentary approval came into force on 21 March 2022.

"Personal Data" means any information that relates to an identified or identifiable natural person, to the extent that such information is protected as personal data under applicable Data Protection Laws and is submitted as Customer Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Standard Contractual Clauses" or sometimes also referred to as the "EU Model Clauses", means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries pursuant to Commission Decision 2021/914/EU of 4 June 2021 or any successor document issued by the European Commission.

"Sub-processor" means any entity engaged by Azeus or a member of the Azeus Group to Process Personal Data in connection with the Services.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the EU GDPR or by the applicable United Kingdom regulator pursuant to the UK Data Protection Act or the UK GDPR.

"Technical and Organizational Measures" means Azeus' Technical and Organizational Measures, as updated from time to time, and currently accessible at https://www.conveneesg.com/legal/tech-and-org-measures.pdf

"Third Country Processor" means any Processor incorporated outside the European Economic Area (EEA) and outside any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data-protection/internationaltransfers/adequacy/index_en.htm (for EEA and Switzerland data exporters), or any Processor incorporated outside any country for which the applicable United Kingdom regulator has published an adequacy decision (for United Kingdom data exporters).

"Third Country Sub-processor" means any Sub-processor incorporated outside the European Economic Area (EEA) and outside any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data-protection/internationaltransfers/adequacy/index_en.htm (for EEA and Switzerland data exporters), or any Processor incorporated outside any country for which the applicable United Kingdom regulator has published an adequacy decision (for United Kingdom data exporters).

"UK GDPR" means the version of the EU GDPR amended by the United Kingdom (UK) authority that is incorporated into UK law and applies in parallel with amended version of the UK Data Protection Act 2018.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Azeus is the Processor and that Azeus or members of the Azeus Group will engage Sub-processors pursuant to the requirements set forth in Section 4 "Sub-processors" below. If Customer is not the sole Controller of the Personal Data, it agrees that it has been instructed by and obtained the authorization of the relevant Controller(s) to agree to the Processing of Customer Personal Data by Azeus as set out in this DPA.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services and provision of instructions, Process Personal Data in accordance with the requirements of applicable Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 **Azeus' Processing of Personal Data.** As Customer's Processor, Azeus shall only Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by End Users in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via emails or support tickets) that are consistent with the terms of the Agreement (individually and collectively, the "**Purpose**"). Azeus acts on behalf of and on the instructions of Customer in carrying out the Purpose.

2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Azeus is the Purpose. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Exhibit A (Description of Processing Activities) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Requests.** Azeus shall, to the extent legally permitted, promptly notify Customer if Azeus receives any requests from a Data Subject to exercise the following Data Subject rights: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a "**Data Subject Request**"). Taking into account the nature of the Processing, Azeus shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Laws.

In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Azeus shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Azeus is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Azeus' provision of such assistance, including any fees associated with provision of additional functionality.

If a Data Subject brings a claim directly against Azeus or its Affiliates for a violation of their Data Subject rights, Customer will indemnify Azeus or its Affiliates for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that Azeus or its Affiliates has notified Customer about the claim and given Customer the opportunity to cooperate with Azeus or its Affiliates in the defense and settlement of the claim. Subject to the terms of the Agreement, Customer may claim from Azeus amounts paid to a Data Subject for a violation of their Data Subject rights caused by Azeus' breach of its obligations under the Data Protection Laws.

4. SUB-PROCESSORS

4.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Azeus' Affiliates may be retained as Sub-processors; and (b) Azeus and Azeus' Affiliates respectively may engage third party Sub-processors in connection with the provision of the Services. As a condition to permitting a third-party Sub-processor to Process Personal Data, Azeus or an Azeus Affiliate will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor.

4.2 List of Current Sub-processors and Notification of New Sub-processors. A current list of Sub-processors for the Services, including the identities of those Sub-processors and their country of location, is accessible via http://www.conveneesg.com/legal/azeus-subprocessors.pdf ("Sub-processor List"). Customer may receive notifications of new Sub-processors by e-mailing dataprocessing_admin@azeus.com with the subject "Subscribe Convene ESG Sub-processor List" and the content "Our company name is: [put down your company name here].", and if a Customer contact subscribes, Azeus shall provide the subscriber with notification of new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

4.3 **Objection Right for New Sub-processors.** Customer may reasonably object to Azeus' use of a new Sub-processor (e.g., if making Personal Data available to the Sub-processor may violate applicable Data Protection Law or weaken the protections for such Personal Data) by notifying Azeus promptly by emailing to dataprocessing@azeus.com within ten (10) business days after receipt of Azeus' notification of use of new Sub-processors. Such notice from Customer shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Azeus will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Azeus is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable Agreement or Order Form(s) with respect only to those Services which cannot be provided by Azeus without the use of the objected-to new Sub-processor by providing written notice to Azeus. Azeus will refund Customer any prepaid fees covering the remainder of the term of such Agreement or Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

4.4 **Liability.** Azeus shall be liable for the acts and omissions of its Sub-processors to the same extent Azeus would be liable if performing the Services of each Sub-processor directly under the terms of this DPA.

5. SECURITY

5.1 **Controls for the Protection of Customer Data.** Azeus shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Technical and Organizational Measures. Azeus regularly monitors compliance with these measures. Azeus will not materially decrease the overall security of the Services during a subscription term.

5.2 **Third-Party Certifications and Audits.** Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Azeus shall make available to Customer (or Customer's independent, third-party auditor) information regarding Azeus' compliance with the obligations set forth in this DPA which can be in the form of the third-party certifications and audits. Customer may contact Azeus in accordance with the "Notices" Section of the

Agreement to request an on-site audit of Azeus' procedures relevant to the protection of Personal Data, but only to the extent required under applicable Data Protection Law. Customer shall reimburse Azeus for any time expended for any such on-site audit at Azeus' then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Azeus shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Azeus or its Affiliates. Customer shall promptly notify Azeus with information regarding any non-compliance discovered during the course of an audit, and Azeus shall use commercially reasonable efforts to address any confirmed non-compliance

6. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

Azeus maintains security measures as specified in the Technical and Organizational Measures. Azeus shall notify Customer of any breach relating to Personal Data (within the meaning of applicable Data Protection Law) of which Azeus becomes aware (a "Customer Data Incident"). Azeus shall provide commercially reasonable cooperation and assistance in identifying the cause of such Customer Data Incident and take commercially reasonable steps to remediate the cause to the extent the remediation is within Azeus' control. The obligations herein shall not apply to incidents that are caused by Customer, End Users and/or any services, software or materials not provided by Azeus or Azeus Group.

7. RETURN AND DELETION OF CUSTOMER DATA

Upon termination of the Services for which Azeus is Processing Personal Data, or after the business purposes for which the Customer Personal Data was collected or transferred have been fulfilled, Azeus shall, upon Customer's request, and subject to any limitations or exceptions described in the Agreement, this DPA or the Technical and Organizational Measures, return all Customer Data and copies of such data to Customer or securely destroy them, unless applicable law prevents it from returning or destroying all or part of Customer Data. Azeus agrees to preserve the confidentiality of any retained Customer Data and will only actively Process such Customer Data in order to comply with the laws it is subject to.

8. CONTROLLER AFFILIATES

8.1 **Contractual Relationship.** The parties acknowledge and agree that, by executing the DPA in accordance with "HOW TO EXECUTE THIS DPA", Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of other Controller(s) including its Controller Affiliates. Each Controller Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Controller Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services by Controller Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Controller Affiliate shall be deemed a violation by Customer.

8.2 **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Azeus under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Controller Affiliates.

8.3 **Rights of Controller Affiliates.** If a Controller Affiliate becomes a party to the DPA with Azeus, it shall, to the extent required under applicable Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

8.3.1 Except where applicable Data Protection Laws require the Controller Affiliate to exercise a right or seek any remedy under this DPA against Azeus directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Controller Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Controller Affiliate individually but in a combined manner for all of its Controller Affiliates together (as set forth, for example, in Section 8.3.2, below).

8.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, if carrying out an on-site audit of the Azeus procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Azeus by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Controller Affiliates in one single audit.

9. LIMITATIONS OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and any and all DPAs between Controller Affiliates and Azeus, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Azeus' and its Affiliates' total liability for all claims from the Customer and all of its Controller Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Controller Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Controller Affiliate that is a contractual party to any such DPA.

10. INTERNATIONAL TRANSFERS

10.1 Limitations on International Transfer (For EU/EEA, Switzerland and United Kingdom). Customer Personal Data from an European Economic Area (EEA), Switzerland or United Kingdom Data Controller(s) may only be exported or accessed by Azeus or its Sub-processors outside the EU/EEA, Switzerland or United Kingdom, as the case may be ("International Transfer"):

(a) if the recipient, or the country or territory in which it processes or accesses Customer Personal Data, ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Customer Personal Data as determined by the European Commission (for EEA or Switzerland data exporters) or by the applicable United Kingdom regulator (for United Kingdom data exporters); or

(b) in accordance with Section 10.2.

10.2 Standard Contractual Clauses and Multi-tier Framework.

(a) The Standard Contractual Clauses, the International Data Transfer Agreement ("IDTA") or any alternative mechanism as approved by the applicable regulator, apply where there is an International Transfer to a country that does not ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Customer Personal Data as determined by the European Commission (for EEA or Switzerland data exporters) or by the applicable United Kingdom regulator (for United Kingdom data exporters).

(b) **Third Country Processor.** Where the Customer is established in the EEA or Switzerland and has signed the Agreement with an Azeus entity that is considered as a Third Country Processor, Standard Contractual Clauses in Exhibit C shall apply, the additional terms of Exhibit B; or any alternative mechanism as approved by the applicable regulator applies.

Where the Customer is established in the United Kingdom and has signed the Agreement with an Azeus entity that is considered as a Third Country Processor, the Parties will execute the IDTA in Exhibit D, the additional terms of Exhibit B; or any alternative mechanism as approved by the applicable regulator applies.

(c) **Third Country Sub-Processor**. For Third Country Sub-processors, Azeus or its Affiliate has entered into the unchanged version of the Standard Contractual Clauses, IDTA or any alternative mechanism as approved by the applicable regulator, prior to the Sub-processor's processing of Customer Personal Data. Customer hereby (itself as well as on behalf of each Controller Affiliates) accede to the applicable Standard Contractual Clauses, IDTA or the alternative mechanism approved by the applicable regulator (as applicable) that is entered into between Azeus and the Third Country Sub-processor. If the Azeus entity that entered into the Agreement with the Customer is not established in the EEA, Switzerland or United Kingdom, the transfer of Customer Personal Data from Azeus (as Processor) to Third Country Sub-processors shall be governed by an agreement providing for the same obligations as those provided in the Standard Contractual Clauses, IDTA or the alternative mechanism entered into between Customer and Azeus, as applicable. Azeus will conduct a transfer impact assessment to properly evaluate the level of protection observed by the Third Country Sub-processors.

(d) Nothing in this DPA will be construed to prevail over any conflicting clause of the Standard Contractual Clauses or the above-mentioned alternative mechanism.

11. UPDATES TO THIS DPA

Azeus may update this DPA when necessary to reflect changes in our Services or to comply with the latest legislation. If Azeus makes any changes, it will notify the Customer by revising the "Published on" date at the top of the DPA and in some cases, where appropriate, Azeus may provide the Customer with additional notice (such as adding a statement to its homepage or sending the Customer an email notification). Any changes will be effective upon posting the revised version of the DPA (or such later effective date as may be indicated at the top of the revised DPA).

12. LEGAL EFFECT

This DPA forms part of the Agreement and is legally binding between Customer and Azeus.

13. GOVERNING LAW & JURISDICTION

As regards what law will apply in any dispute or lawsuit arising out of or in connection with this DPA, and which courts have jurisdiction over any such dispute or lawsuit, the parties agree to follow the same governing law and jurisdiction as agreed in the Agreement.

List of Exhibits

Exhibit A: Description of Processing Activities

Exhibit B: Additional Data Transfer Terms

Exhibit C: Standard Contractual Clauses (processors)

Exhibit D: International Data Transfer Agreement

Exhibit A - Description of Processing Activities

General – Subject matter of the Processing

The context for the Processing of Customer Personal Data is as specified in the Agreement which is mainly Azeus' provision of the Services, which shall involve performance on behalf of Customer of the tasks and activities set out in the Agreement.

Nature and Purpose of the Processing

The nature and purposes of the Processing of Customer Personal Data carried out by Azeus on behalf of Customer shall be as set out in the Agreement, which in particular shall be for Customer to receive the Services under the Agreement, and not for any new purpose other than those previously approved.

Data subjects

Customer may submit Personal Data to the Services or to Azeus in relation to the Agreement, the extent of which is determined and controlled by Customer and which may include, but is not limited to, Personal Data relating to the following categories of data subject:

- End Users including collaborators;
- employees of Customer;
- directors of Customer;
- trustees of Customer;
- consultants of Customer;
- contractors of Customer;
- agents of Customer;
- suppliers and services providers of Customer; and/or
- third parties with which Customer conducts business.

Categories of data

The Personal Data transferred concern the following categories of data:

Any Personal Data comprised in Customer Data. This may include, for example,

- User accounts – End Users including collaborators
- Authors of reporting materials
- Customer staff and others referred to in the reporting materials
- Communication history with support helpdesk (e.g. emails, conversations)
- Contact information for billing and contract management purposes

Any Personal Data which we may collect as specified in the Convene ESG Privacy Policy at http://www.conveneesg.com/privacypolicy/ .

In principle, other categories of data relevant to the delivery of the Services or the Agreement may be added.

Special categories of data

Azeus does not require any special categories of data to provide the Services. If Customer store or upload documents which concerns special categories of data, same as all other documents, it is encrypted during both during storage and in transit.

Processing operations

The Personal Data transferred will be processed in accordance with the Agreement and any Order Form and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain, and improve the Services provided to Customer;
- guide the Customer in the preparation of their ESG reports as part of the Services
- to provide customer support, helpdesk or technical support to Customer;
- to notify Customer about changes to our Services;
- to communication with Customer regarding news or updates about Azeus Group and Convene ESG;
- billing and contract management; and
- disclosures in accordance with the Agreement, as compelled by law.

Duration of Processing

Customers and their End Users with an active subscription of the Services have complete control over how long the Content (e.g. raw monthly data for ESG report compilation) they uploaded to Convene ESG is stored in the servers and can delete such Content from their accounts at any time during the term of their subscription.

Processing of the Customer Personal Data by Azeus shall be for the term of the Agreement for the purpose of and only to the extent required as set out in the Agreement, provided that Customer Personal Data shall not be Processed for longer than is necessary for the purpose for which it was collected or is being Processed (except where a statutory exception applies) subject to the following:

- Customer must inform Azeus within 30 days after termination of the Agreement if there are any data, they want to retrieve beyond which Azeus has no obligation to maintain any data stored in the Customer's account or environment.
- Customer registration information, contracts, agreements and billing information will be kept by Azeus beyond the end of the Agreement. Such information constitutes Azeus' business records and is kept to comply with Azeus' financial and audit policies, as well as tax requirements.
- Documentation intended as proof of proper data processing will be kept by Azeus beyond the end of the Agreement.
- Support information is retained to ensure efficient support in case of recurring issues and to comply with Azeus' audit policies related to business records of services provided to Customers. Customers may request deletion of such information containing their Personal Data via email to dataprocessing@azeus.com.
- Data in systems (such as email systems) which are used for many Customers and in respect of which the separation of the data of a Customer would be disproportionately burdensome, are archived and/or deleted at cyclical periods. Customers may request deletion of such information containing their Personal Data via email to dataprocessing@azeus.com.
- Azeus may retain data necessary for its legal purposes.

Exhibit B - Additional Data Transfer Terms

1. **Customers covered by the Standard Contractual Clauses or the International Data Transfer Agreement, as applicable.** The Standard Contractual Clauses, International Data Transfer Agreement and the additional terms specified in this Exhibit B apply to (i) the legal entity that has executed the Standard Contractual Clauses or International Data Transfer Agreement (as applicable) as a data exporter and its Controller Affiliates and, (ii) all Affiliates of Customer established within the European Economic Area, Switzerland or the United Kingdom, which have signed Order Forms for the Services.

2. **Instructions.** This DPA and the Agreement are Customer's complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. The following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by End Users in their use of the Services; and (c) Processing to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) where such instructions are consistent with the terms of the Agreement.

3. **Appointment of new Sub-processors and List of current Sub-processors.** Customer acknowledges and expressly agrees that (a) Azeus' Affiliates may be retained as Sub-processors; and (b) Azeus and Azeus' Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Azeus shall make available to Customer the current list of Sub-processors in accordance with Section 4.2 of this DPA.

4. **Notification of New Sub-processors and Objection Right for new Sub-processors.** Customer acknowledges and expressly agrees that Azeus may engage new Sub-processors as described in Sections 4.2 and 4.3 of the DPA.

5. **Copies of Sub-processor Agreements.** The parties agree that any copies of the Sub-processor agreements that are provided by Azeus to Customer may have all commercial information, or clauses unrelated to the Standard Contractual Clauses, International Data Transfer Agreement or their equivalent, removed by Azeus beforehand; and, that such copies will be provided by Azeus, in a manner to be determined in its discretion, only upon request by Customer.

6. **Audits and Certifications.** The parties agree that audits to demonstrate compliance with the obligations set out in Standard Contractual Clauses or International Data Transfer Agreement (as applicable) shall be carried out in accordance with the following specifications: Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Azeus shall make available to Customer (or Customer's independent, third-party auditor) information regarding Azeus' compliance with the obligations set forth in this DPA which can be in the form of the third-party certifications and audits. Customer may contact Azeus in accordance with the "Notices" Section of the Agreement to request an on-site audit of Azeus' procedures relevant to the protection of Personal Data, but only to the extent required under applicable Data Protection Law. Customer shall reimburse Azeus for any time expended for any such on-site audit at the Azeus Group's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Azeus shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Azeus. Customer shall promptly notify Azeus with information regarding any non-compliance discovered during the course of an audit, and Azeus shall use commercially reasonable efforts to address any confirmed non-compliance.

7. **Conflict.** In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses or the International Data Transfer Agreement) and the Standard Contractual Clauses in Exhibit C or the International Data Transfer Agreement (as applicable), the Standard Contractual Clauses or the International Data Transfer Agreement (as applicable) shall prevail.

Exhibit C - Standard Contractual Clauses (processors)

FOR EU/EEA and Switzerland:

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

Name of the data exporting organisation: .....

Address: .....

Tel.: .....; fax: .....; e-mail: .....

Other information needed to identify the organisation:

.....

(the data **exporter**)

And

Name of the data importing organisation: **The Azeus entity that entered into the Agreement with the Customer**

Address: **As indicated in the Agreement**

Email: **legal@azeus.com**

Other information needed to identify the organisation:

.....

(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.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal 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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 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 [...].

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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

Not Used

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 its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be

obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

---

[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.

(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) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

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

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

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

---

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

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 Ireland.

Clause 18

Choice of forum and jurisdiction

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

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

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter:

Name: The entity identified as Customer in the DPA.

Address: The address for Customer associated with its Convene ESG account or as otherwise or as otherwise specified in the DPA or the Agreement.

Contact person's name, position and contact details: The contact details associated with Customer's account, or as otherwise specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Exhibit A of the DPA

Signature and date: By using the Services to transfer Customer Data to Third Countries, the data exporter will be deemed to have signed this Annex I.

Role (controller/processor): Controller

Data importer(s):

Name: Azeus as identified in the DPA and the Agreement.

Address: The Address for Azeus specified in the Agreement

Contact person's name, position and contact details: The contact details for Azeus specified in the DPA or the Agreement

Activities relevant to the data transferred under these Clauses: The activities specified in Exhibit A of the DPA

Signature and date: By transferring Customer Data to Third Parties on Customer's instructions, 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

Categories of data subjects are specified in Exhibit A of the DPA

Categories of personal data transferred

The personal data is described in Exhibit A of the DPA

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff

having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Azeus does not require any special categories of data to provide the Services. If Customer store or upload documents which concerns special categories of data, same as all other documents, it is encrypted during both during storage and in transit. Only the Customer or End Users are entitled to access, retrieve and direct the use of such information.The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Nature of the processing

The nature of the processing is described in Exhibit A of the DPA

Purpose(s) of the data transfer and further processing

Purpose of data transfer and further processing is described in Exhibit A of the DPA

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

Such period is described in Exhibit A of the DPA

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

Such matters are described in Exhibit A of the DPA

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 accodance 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 organisational 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.

> Azeus has implemented and shall maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Customer Data, as set forth in the Technical and Organizational Measures, which is currently accessible at https://www.conveneesg.com/legal/tech-and-org-measures.pdf .

For transfers to (sub-) processors, also describe the specific technical and organisational 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

Sub-processors are required to provide at least the same standard of technical and organizational measures as Azeus.

Exhibit D – International data transfer agreement

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

1. International Data Transfer Agreement

VERSION A1.0, in force 21 March 2022

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

2. Part 1: Tables

Part 1 Table 1: Parties and signatures

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Customer Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Azeus Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:

Importer Data Subject Contact		Job Title: Contact details including email:
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the **Exporter** set out above Signed: Date of signature: Full name: Job title:	Signed for and on behalf of the **Importer** set out above Signed: Date of signature: Full name: Job title:

Part 2 **Table 2: Transfer Details**

UK country's law that governs the IDTA:	☒ England and Wales ☐ Northern Ireland ☐ Scotland
Primary place for legal claims to be made by the Parties	☒ England and Wales ☐ Northern Ireland ☐ Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ☒ Exporter is a Controller ☐ Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: ☐ Importer is a Controller ☒ Importer is the Exporter's Processor or Sub-Processor ☐ Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	☒ UK GDPR applies to the Importer's Processing of the Transferred Data ☐ UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the Agreement (including this DPA)

	Other agreements – N/A **If the Exporter is a Processor or Sub-Processor** – N/A
Term	The Importer may Process the Transferred Data for the following time period: ☐ the period for which the Linked Agreement is in force ☒ time period: see Exhibit A of this DPA ☐ (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	☒ the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. ☐ the Parties can end the IDTA before the end of the Term by serving: ____ months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: ☒ Importer ☒ Exporter ☐ neither Party
Can the Importer make further transfers of the Transferred Data?	☒ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). ☐ The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ☐ if the Exporter tells it in writing that it may do so. ☐ to: ____ ☐ to the authorised receivers (or the categories of authorised receivers) set out in: ☒ there are no specific restrictions.
Review Dates	☐ No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: ____ The Parties must review the Security Requirements at least once: ☐ each ____ month(s)

	☐ each quarter ☐ each 6 months ☐ each year ☐ each _____ year(s) ☒ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

Part 3 Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: ☒ The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: ☐ racial or ethnic origin ☐ political opinions ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic data ☐ biometric data for the purpose of uniquely identifying a natural person ☐ physical or mental health ☐ sex life or sexual orientation ☐ criminal convictions and offences ☒ none of the above ☐ set out in: And: ☒ The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Relevant Data Subjects	The Data Subjects of the Transferred Data are:

	☒ The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Purpose	☐ The Importer may Process the Transferred Data for the following purposes: ☒ The Importer may Process the Transferred Data for the purposes set out in: see Exhibit A of this DPA In both cases, any other purposes which are compatible with the purposes set out above. ☒ The purposes will update automatically if the information is updated in the Linked Agreement referred to. ☐ The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 4 Table 4: Security Requirements

Security of Transmission	Please refer to the Convene ESG Technical and Organisational Measures document available at https://www.conveneesg.com/legal/tech-and-org-measures.pdf .
Security of Storage	Please see the above.
Security of Processing	Please see the above.
Organisational security measures	Please see the above.
Technical security minimum requirements	Please see the above.
Updates to the Security Requirements	☒ The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. ☐ The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

3. Part 2: Extra Protection Clauses

Extra Protection Clauses:	
(i) Extra technical security protections	
(ii) Extra organisational protections	
(iii) Extra contractual protections	

4. Part 3: Commercial Clauses

Commercial Clauses	

5. Part 4: Mandatory Clauses

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.