IPSOFT / AMELIA DATA PROCESSING AGREEMENT

Last Modified: 21 April 2022

NOTE:

The IPsoft / Amelia Data Processing Agreement is made available at *https://amelia.ai/legal/ipsoft-amelia-dpa/* and is incorporated into Master Framework Agreement or other written or electronic agreement between IPsoft / Amelia and Customer (the "Agreement") for the purchase of IPsoft / Amelia products and services (including associated offline or mobile components) from IPsoft / Amelia (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") to reflect the parties' agreement with regard to the Processing of Personal Data.

For Customers that would like to receive a signed copy of the IPsoft / Amelia Data Processing Agreement, we have made this copy available to you. This copy includes signatures on the Data Processing Agreement version last modified as indicated above.

How to Complete this Data Processing Agreement

1. This DPA has been pre-signed by the appropriate IPsoft/Amelia party.
2. To complete this DPA, Customer must complete the signature boxes on page (as applicable depending on whether and which standard contractual clauses need to be agreed) 7, 19, 36, 37 and 38.
3. Submit the completed and signed DPA to us at *datatransfers@amelia.com* providing a return email address. Please provide a copy of your agreement with IPsoft/Amelia or the name of the IPsoft/Amelia entity you have a contract with and an agreement reference (if available).
4. We will confirm and return the DPA to the Customer. Upon submitting the validly completed DPA to the email address provided by the Customer, this DPA will become legally binding.

No changes made to this copy are agreed to by IPsoft Incorporated, Amelia US LLC, IPsoft EU Holding B.V., Amelia NL B.V., or its/their affiliates.

Please note that we update the Data Processing Agreement as we describe in the 'General Provisions' section below. Current Data Processing Agreement terms are available at *https://amelia.ai/legal/ipsoft-amelia-dpa/* and archived Data Processing Agreement terms are available at *https://amelia.ai/legal/ipsoft-amelia-dpa/* . If you have any questions, please contact your IPsoft / Amelia representative.

- This IPsoft / Amelia Data Processing Agreement and its Annexes ("DPA") reflects the parties' agreement with respect to the Processing of Personal Data by us on behalf of you in connection with the agreement between you and us (also referred to in this DPA as the "Agreement").
- This DPA is supplemental to, and forms an integral part of, the Agreement and is effective upon its incorporation into the Agreement, which may be specified in the Agreement, an Order, or an executed amendment to the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.
- We update these terms from time to time by placing a notice on this site. You can find archived versions of the DPA at the bottom of this page when the document is updated.
- The term of this DPA will follow the term of the Agreement. Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

I. Definitions.

- "**California Personal Information**" means Personal Data that is subject to the protection of the CCPA.

- "**CCPA**" means California Civil Code Sec. 1798.100 et seq., also known as the California Consumer Privacy Act of 2018.
- "**Consumer**", "**Business**", "**Sell**", and "**Service Provider**" will have the meanings given to them in the CCPA.
- "**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.
- "**Data Protection Laws**" means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, the CCPA and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated or replaced from time to time.
- "**Data Subject**" means the individual to whom Personal Data relates.
- "**Europe**" means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.
- "**European Data**" means Personal Data that is subject to the protection of European Data Protection Laws.
- "**European Data Protection Laws**" means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union ("UK GDPR"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case, as may be amended, superseded or replaced ("Swiss Data Protection Law").
- "**Instructions**" means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available). If you are a Processor, "Instructions" refers to the Controller's written, documented instructions forwarded by you to us.
- "**Permitted Affiliates**" means any of your Affiliates that (i) are permitted to use the Subscription Services pursuant to the Agreement, but have not signed their own separate agreement with us and are not a "Customer" as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by us, and (iii) are subject to European Data Protection Laws.
- "**Personal Data**" means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data, personal information, or personally identifiable information under applicable Data Protection Laws.
- "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Subscription Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- "**Privacy Shield**" means the EU-U.S. and Swiss-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to its Decision of July, 12 2016 but invalidated by the judgment of the Court of Justice of the EU in Case C-311/18 (*Schrems II*) and approved by the Swiss Federal Council on January 11, 2017 respectively; as may be amended, superseded or replaced.
- "**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of July 12, 2016; as may be amended, superseded, or replaced.
- "**Processing**" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly.
- "**Processor**" means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.
- "**Standard Contractual Clauses**" means the standard contractual clauses approved pursuant to the European Commission's Decision
    - (EU) 2021/914 of 4 June 2021 with respect to Personal Data subject to the GDPR, in the form set out at
        - Annex C (Module Two for transfers from controllers to processors) and
        - Annex D (Module Three for transfers from processors to processors);

as may be amended, superseded or replaced ("Standard Contractual Clauses 2021");

  - (C(2010)593) of 5 February 2010 with respect to Personal data subject to UK GDPR/Swiss Data Protection Law, in the form set out at Annex E; as may be amended, superseded or replaced ("Standard Contractual Clauses 2010").

- "**Sub-Processor**" means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the Subscription Services under the Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any IPsoft/Amelia employee or consultant.

II. Customer Responsibilities

a) Compliance with Laws. Within the scope of the Agreement and in its use of the services, you will be responsible for complying with all requirements that apply to you under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions you issue to us.

In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which you acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly your use for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Services, including those relating to obtaining consents (where required). You will inform us without undue delay if you are not able to comply with your responsibilities under this sub-section a) or applicable Data Protection Laws.

b) Controller Instructions. The parties agree that the Agreement (including this DPA), together with your use of the Subscription Services in accordance with the Agreement, constitute your complete and final Instructions to us in relation to the Processing of Personal Data, and additional instructions outside the scope of the Instructions shall require prior written agreement between us and you.

III. IPsoft/Amelia Obligations

a) Compliance with Instructions. We will only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful documented Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

b) Conflict of Laws. If we become aware that we cannot Process Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Agreement for any failure to perform the applicable Services until such time as you issue new lawful Instructions with regard to the Processing.

c) Security. We will implement and maintain appropriate technical and organizational measures to ensure the security of the Personal Data, including protection against Personal Data Breaches, as described under Annex B to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a degradation in the protection offered by the Security Measures.

d) Confidentiality. We will ensure that any personnel whom we authorize to Process Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

e) Personal Data Breaches. We will notify you without undue delay after we become aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance, i.e. taking into account the nature and Processing and the information available to us, as necessary to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects (or, in case you are a Processor, the Controller), if you are (or, in case you are a Processor, the Controller is) required to do so under Data Protection Laws.

f) Deletion or Return of Personal Data. We will delete or return all Customer Data, including Personal Data (including copies thereof) Processed pursuant to this DPA, on termination or expiration of your Service in accordance with the procedures and timeframes set out in the Agreement, save that this requirement shall not apply to the extent we are required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with its deletion practices. You may request the deletion of your account(s) after expiration or termination of your subscription by submitting a request in our Data Subject Portal (*https://app.onetrust.com/app/#/webform/9282f952-0743-4bcd-bd2c-9e6eba16424b*) or by contacting your IPsoft/Amelia representative.

IV. Data Subject Requests.

a) The Services provide you with a number of controls that you can use to retrieve, correct, delete or restrict Personal Data, which you can use to assist you in connection with your obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

b) To the extent that you are unable to independently address a Data Subject Request through the Service, then upon your written request we will provide reasonable assistance to you to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Agreement. You shall reimburse us for the commercially reasonable costs arising from this assistance.

c) If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to us, we will promptly inform you and will advise the Data Subject to submit their request to you. You will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data.

V. Sub-Processors.

You agree that we may engage Sub-Processors to Process Personal Data on your behalf (or on behalf of the Controller should you be a Processor). We have currently appointed, as Sub-Processors, the Amelia Affiliates and third parties listed in Annex F to this DPA. We will notify you if we add or remove Sub-Processors to Annex F prior to any such changes.

Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under this DPA.

VI. Data Transfers.

You acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Service in accordance with the Agreement, and in particular that Personal Data may be transferred to the United States and to other jurisdictions where IPsoft/Amelia Affiliates and Sub-Processors have operations in order to meet and comply with our support obligations. We will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

VII. Additional Provisions for European Data.

a) Scope of Section VII. This "Additional Provisions for European Data" section shall apply only with respect to European Data.

b) Roles of the Parties. When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that you are either the Controller of European Data and we are the Processor or that you are the Processor of European Data and we are the Sub-Processor.

c) Instructions. If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay. Where we are obligated to Process Personal Data based on applicable law (i.e. independent of your instructions), we will inform you of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

d) Personal Data Breaches: Information on Personal Data Breaches relevant to the Personal Data Processed on your behalf will be made available to you as it becomes known without undue delay.

e) Deletion or Return of Personal Data: Whether the Personal Data will be returned or deleted depends on your choice.

f) Notification and Objection to New Sub-Processors. We will notify you in writing of any changes to Sub-processors by updating Annex F to this DPA and providing this update to you and will give you the opportunity to object to such changes within 30 days after updating Annex F to this DPA and providing this update to you. If you object to changes to Sub-Processors based on reasonable grounds, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected Service(s) in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination).

g) Security of Processing, Data Protection Impact Assessments and Consultation with Supervisory Authorities. We will provide reasonable assistance to you with respect to compliance with obligations related to the security of processing. To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws.

h) Transfer Mechanisms for Data Transfers.

1) IPsoft / Amelia shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation and as recognized by European Data Protection Laws) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

2) You acknowledge that in connection with the performance of the Subscription Services, IPsoft Incorporated/Amelia US LLC is a recipient of European Data in the United States.

3) The parties acknowledge and agree the following:

i) *Standard Contractual Clauses*: IPsoft Incorporated/Amelia US LLC agrees to abide by and process European Data in compliance with the appropriate Standard Contractual Clauses:

- Standard Contractual Clauses 2021 (Module Two) in Annex C to the DPA where you are Controller and IPsoft Incorporated/Amelia US LLC is Processor;

- Standard Contractual Clauses 2021 (Module Three) in Annex D to the DPA where you are a Processor and IPsoft Incorporated/Amelia US LLC is Processor;

- Standard Contractual Clauses 2021 (Module Three) in Annex D to the DPA where you are Controller, an IPsoft / Amelia contracting entity under the Agreement which is located in the EU is Processor and IPsoft Incorporated/Amelia US LLC is Sub-Processor (note: you will not be a party to these Standard Contractual Clauses which will be concluded between the IPsoft / Amelia contracting entity under the Agreement which is located in the EU and IPsoft Incorporated/Amelia US LLC);

- Standard Contractual Clauses 2021 (Module Three) in Annex D to the DPA where you are Processor, an IPsoft / Amelia contracting entity under the Agreement which is located in the EU is Sub-Processor and IPsoft Incorporated/Amelia US LLC is Sub-Sub-Processor (note: you will not be a party to these Standard Contractual Clauses which will be concluded between the IPsoft / Amelia contracting entity under the Agreement which is located in the EU and IPsoft Incorporated/Amelia US LLC);

- Standard Contractual Clauses 2010 in Annex E to the DPA where UK GDPR or Swiss Data Protection Law is applicable to the Personal Data Processed on behalf of you (or on behalf of the Controller, if you are a Processor).

For the avoidance of doubt, Standard Contractual Clauses shall only be agreed on where this is required under European Data Protection Laws.

ii) *Privacy Shield*: Although IPsoft Incorporated and its Affiliates do not rely on the EU-US Privacy Shield as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18 (*Schrems II*), for as long as IPsoft Incorporated is self-certified to the Privacy Shield, IPsoft Incorporated (and its US-based Affiliates, including Amelia US LLC) will process European Data in compliance with the Privacy Shield Principles and let you know if it is unable to comply with this requirement.

4) The parties agree that

i) purely for the purposes of the descriptions in the Standard Contractual Clauses, Amelia US LLC will be deemed the “data importer” and Customer will be deemed the “data exporter” where your Agreement is with IPsoft Incorporated or Amelia US LLC (notwithstanding that you may yourself be located outside Europe and/or be acting as Processor on behalf of a Controller),

ii) notwithstanding the foregoing, where UK GDPR or Swiss Data Protection Law is applicable to the Personal Data Processed on behalf of you (or on behalf of the Controller, if you are a Processor) and the IPsoft / Amelia contracting entity under the Agreement is located in the EU, you provide such contracting entity with a mandate (if you are a Processor: a mandate of the Controller) to enter into the Standard Contractual Clauses 2010 with IPsoft Incorporated / Amelia US LLC in your name and on your behalf (if you are a Processor: in the name and on behalf of the Controller); such contracting entity will remain fully and solely responsible and liable to you for the performance of the Standard Contractual Clauses 2010 by IPsoft

Incorporated / Amelia US LLC, and you will direct any instructions, claims or enquiries in relation to the Standard Contractual Clauses to such contracting entity (not to IPsoft Incorporated or Amelia US LLC); and

iii) if and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

i) Demonstration of Compliance. We will make all information reasonably necessary to demonstrate compliance with this DPA, including the Standard Contractual Clauses (where applicable), available to you and allow for and contribute to audits, including inspections by you to assess compliance with this DPA. You may choose to conduct such audit by yourself or mandate an independent auditor. You acknowledge and agree that you will exercise your audit rights under this DPA by instructing us to comply with the audit measures described in this sub-section g). You acknowledge that the Subscription Services are hosted by our data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are regularly tested by independent third-party penetration testing firms. Upon request, we will supply (on a confidential basis) a summary copy of its penetration testing report(s) to you so that you can verify our compliance with this DPA. Further, at your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will exercise this right at reasonable intervals (i.e. typically not more than once per calendar year) or if there are indications of non-compliance.

VIII. Additional Provisions for California Personal Information.

a) Scope of this Section VIII. The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

b) Roles of the Parties. When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business and we are a Service Provider for the purposes of the CCPA.

c) Responsibilities. The parties agree that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services (whether product or professional) under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA.

IX. General Provisions.

a) Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to the “Compliance with Instructions” or “Security” sections of this DPA, we reserve the right to make any updates and changes to this DPA and the terms that apply in relevant modification section (regardless of name) of the Agreement will apply.

b) Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

c) Limitation of Liability. Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the parties) and the Standard Contractual Clauses (where applicable and to the extent permissible under these Standard Contractual Clauses), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the “Limitation of Liability” section of the Master Agreement and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA). For the avoidance of doubt, if Amelia US LLC is not a party to the Agreement, the “Limitation of Liability” section of the Master Agreement will apply as between you and Amelia US LLC, and in such respect any references to “IPsoft,” “Amelia,” “we,” “us,” or “our” will include both Amelia US LLC and the IPsoft / Amelia entity that is a party to the Agreement. For the avoidance of doubt, with respect to Personal Data to which European Data Protection Laws apply, the direct liability towards Data Subjects shall not be limited through this.

d) Governing Law. As applicable, the Standard Contractual Clauses 2021 shall be governed by the law specified in Clause 17 therein and the Standard Contractual Clauses 2010 in accordance with Clause 9 therein. Otherwise, this DPA will be governed by and construed in accordance with:

1) If your Agreement is with IPsoft Incorporated or Amelia US LLC, the governing law is the law of the State of New York and applicable law of the United States, with exclusive jurisdiction in the State of New York, and exclusive forum of either the United States District Court for the Southern District of New York OR the New York State Supreme Court, Commercial Division, Manhattan (as applicable); or

2) If your Agreement is with IPsoft EU Holding, Amelia NL B.V., the governing law is the law of the Netherlands and applicable European Union law, with exclusive jurisdiction in Amsterdam, the Netherlands, and exclusive forum of the Netherlands Commercial Court and if not available, the Amsterdam District Court.

The selection of governing law, jurisdiction, and forum will apply unless required otherwise by Data Protection Laws.

X. Parties to this DPA.

a) Permitted Affiliates. By signing the Agreement, you enter into this DPA on behalf of yourself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of your Permitted Affiliates, thereby establishing a separate DPA between us and each such Permitted Affiliate subject to the Agreement and the ‘General Provisions’ and ‘Parties to this DPA’ sections of this DPA. Each Permitted Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the purposes of this DPA only, and except where indicated otherwise, the terms “Customer”, “you” and “your” will include you and such Permitted Affiliates.

b) Authorization. The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c) Remedies. Except where applicable Data Protection Laws require a Permitted Affiliate to exercise a right or seek any remedy under this DPA against us directly by itself, the parties agree that (i) solely the Customer entity that is the contracting party to the Agreement will exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all communication with us under the DPA and will be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

d) Other rights. The parties agree that you will, when reviewing our compliance with this DPA pursuant to the “Demonstration of Compliance” section, take all reasonable measures to limit any impact on us and our Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Agreement and all of its Permitted Affiliates in one single audit.

EXECUTED BY THE PARTIES AUTHORIZED REPRESENTATIVES:

IPsoft Incorporated / Amelia US LLC, by and on their own or by and on behalf of their affiliates, as applicable.	**Customer:**
Name (full): Jeffrey Neu	Name (full): ____
Position: Chief Legal Officer	Position: ____
	Date: ____
Signature:	Signature:

Annex A Details of Processing

This Annex A forms part of the DPA.

A. **Nature and Purpose of Processing.** We will Process Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in the applicable Order Form, and as further instructed by you in your use of the Services.

B. **Duration of Processing.** Subject to the "Deletion or Return of Personal Data" section of this DPA, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

C. **Categories of Data subjects.** You may submit Personal Data in the course of using the Services, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

   a. Your users and other end users including your employees, contractors, collaborators, customers, prospects, suppliers, and subcontractors.

   b. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to your end users.

   c. Your users who are authorized by you to use the Services.

D. **Categories of Personal Data.** You may submit Personal Data to the Services, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data:

   a. Names, Titles, Positions, and Employer Information

E. Contact Information, such as email addresses, work addresses, and other physical location data,

F. Connection data related to the access to the Services, except to the extent that such data is anonymized or pseudonymized,

   a. Conversation data related to the usage of the Services, except to the extent that such data is anonymized or pseudonymized,

   b. Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Services.

G. **Special categories of data (if appropriate).** The parties do not anticipate the transfer of special categories of data.

H. **Processing operations.** Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

   a. Storage and other Processing necessary to provide, maintain, and improve the Services provided to you; and/or

   b. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

ANNEX B Security Measures

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

4.1 Measures of pseudonymization and encryption of personal data.

4.1.1 IPsoft Amelia LLC requires full-disk hard drive encryption using AES-256 for all employee computers, and uses role-based access control ("RBAC"), multi-factor authentication ("MFA"), and account management procedures to control access to Customer Data.

4.1.2 IPsoft Amelia LLC encrypts data in transit and at rest using hybrid encryption techniques that constitute software-based encryption, hosting solutions (e.g. Amazon Web Services ("AWS")), and self-encrypting drives to align with NIST Special Publication 800-53.

4.1.3 Customer Data at rest is encrypted using the AES-256 algorithm.

4.1.4 IPsoft Amelia LLC uses Transport Layer Security ("TLS") protocol version 1.2 or higher to protect HTTPS communications.

4.1.5 For email security, IPsoft Amelia LLC leverages opportunistic TLS encryption (OE) by default.

4.1.6 Customer Data that resides in AWS is encrypted at rest as stated in AWS's documentation and whitepaper. Further information about AWS's security practices can be found at https://aws.amazon.com/compliance/data-center/controls/.

4.1.7 AWS log-in credentials and private keys generated by the Service are for IPsoft Amelia LLC's internal use only.

4.1.8 Encryption keys are rotated.

4.2 Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services.

4.2.1 IPsoft Amelia LLC maintains a record of personnel authorized to access systems that contain Customer Data.

4.2.2 Privileged access requires a formal account management and access control procedure that requires review and approval from a line manager or other executives, as dictated by IPsoft Amelia LLC's information security policies.

4.2.3 IPsoft Amelia LLC deactivates authentication credentials of individuals promptly following the date of their employment or services termination or a role transfer that no longer requires access to Customer Data.

4.2.4 IPsoft Amelia LLC's personnel are legally obligated to maintain the confidentiality of Customer Data and this obligation continues even after their employment or services provided end.

4.2.5 Employees complete mandatory training annually, which covers data privacy and governance, data protection, confidentiality, social engineering, password policies, and information security.

4.2.6 IPsoft Amelia LLC requires difficult-to-guess passwords for all employees and follows NIST best practices.

4.2.7 IPsoft Amelia LLC web application account passwords are hashed when stored.

4.2.8 IPsoft Amelia LLC web application sessions expire after 30 minutes of inactivity to prevent further access to the system.

4.2.9 The IPsoft Amelia LLC web application retains session locks until the session user reestablishes access using IPsoft Amelia LLC identification and authorization procedures.

4.3 Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

4.3.1 IPsoft Amelia LLC maintains geographically-distributed data centers leveraging AWS cloud hosting infrastructure in several jurisdictions, including the United States (US East and West Regions), Canada (Central Region), Australia (Asia Pacific, Sydney Region), the United Kingdom (London Region), and the EU (Frankfurt Region).

4.3.2 IPsoft Amelia LLC's information systems have security controls designed to detect and mitigate attacks by using logs and alerting.

4.3.4 IPsoft Amelia LLC's incident reporting and response procedure aligns with NIST SP 800-61 guidance on handling incidents, including steps for breach notification.

4.3.5 All incidents are logged in an incident tracking system that is subject to auditing on an annual basis.

4.3.6 IPsoft Amelia LLC has a business continuity and disaster recovery plan that incorporates input from periodic risk assessments, vulnerability scanning, and threat analysis.

4.3.7 IPsoft Amelia LLC conducts an incident response and business continuity and disaster recovery test annually that is used to inform the ongoing risk assessment and management process.

4.4 Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.

4.4.1 IPsoft Amelia LLC conducts regular risk assessments and monitors the effectiveness of its safeguards, controls, and systems, including conducting vulnerability scanning, annual penetration testing, intrusion detection, and continuous monitoring.

4.4.2 IPsoft Amelia LLC's vulnerability management program includes an independent testing team to perform vulnerability scanning and a variety of vulnerability scanning tools to assess its internal and external network environments against emerging security threats.

4.4.3 IPsoft Amelia LLC implements server protection on the production environment and endpoint protection on laptop/desktop endpoints, including antivirus, which are continuously updated with critical patches or security releases.

4.4.4 The servers that host the IPsoft Amelia LLC Service are scanned for viruses and malware on a weekly basis.

4.4.5 The IPsoft Amelia LLC web application, network segmentation, and interconnections are protected by firewalls.

4.4.6 The Amazon Virtual Private Cloud ("VPC") allows IPsoft Amelia LLC services to operate in separate, virtual networks that are isolated from other external traffic.

4.4.7 IPsoft Amelia LLC's corporate equipment is protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access.

4.4.8 Sub-processors undergo onboarding due diligence to ensure compliance with security and privacy requirements, laws, and regulations. In addition and to the extent applicable, sub-processors are required to sign a Data Processing Addendum (DPA) that includes compliance with data protection laws, confidentiality, data retention, and access requirements.

4.5 Measures for user identification and authorization.

4.5.1 IPsoft Amelia LLC uses commercially reasonable practices to identify and authenticate users who attempt to access information systems. IPsoft Amelia LLC's authentication and password protection practices are designed to maintain the confidentiality and integrity of account credentials when they are assigned and distributed and during storage.

4.5.2 Customers are able to set their own password complexity as well as enable Single Sign On via the SAML 2.0 protocol

4.6 Measures for the protection of Customer Data during transmission.

4.6.1 Customer Data is encrypted in transit. Encryption is a requirement.

4.6.2 All communications between the Customer and IPsoft Amelia LLC, as well as all third-party applications, take place over a secure HTTPS connection using TLS 1.2 or higher protocol to ensure data in transit is encrypted.

4.6.3 The IPsoft Amelia LLC production environments include logical and physical separation of components using networking and software defined networking technologies where appropriate. Production, testing, and staging environments are also logically separated to ensure the security of Customer Data.

4.6.4 All connections between IPsoft Amelia LLC internal networks and the Internet or any other publicly-accessible computer network include an approved firewall or related access control system.

4.7 Measures for the protection of Customer Data during storage.

4.7.1 Customer Data is hosted by AWS. IPsoft Amelia LLC maintains complete administrative control over its virtual servers.

4.7.2 AWS Key Management System ("KMS") managed server-side encryption keys are used to encrypt data in our cloud infrastructure. AWS KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to protect keys that cannot be retrieved from the service by anyone or transmitted beyond the AWS regions where they were created.

4.7.3 Customer Data within IPsoft Amelia LLC's multi-tenant environments is logically segregated and attempts to access Customer Data outside allowed domain boundaries are prevented and logged (Customer Data can be logically and physically segregated in accordance with the Customer Agreement).

4.7.4 The IPsoft Amelia LLC web application runs antivirus scans regularly to detect malicious files present in the production environment and all personal data access is logged.

4.7.5 Customer Data is protected during storage by AWS endpoint protection, which includes firewalls and antivirus.

4.8 Measures for ensuring physical security of locations where Customer Data is processed.

4.8.1 Physical access to data hosting facilities is documented and managed by AWS.

4.8.2 IPsoft Amelia LLC limits access to its corporate offices to identified authorized individuals who require access for the performance of their job function and authorized visitors.

4.8.3 All visitors to IPsoft Amelia LLC's corporate offices are escorted at all times by authorized personnel.

4.8.4 Physical access to IPsoft Amelia LLC's corporate offices is managed and administered by the Business Operations team.

4.8.5 IPsoft Amelia LLC uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or disruptions to IPsoft Amelia LLC's corporate office.

4.8.6 Access to customer physical media is limited to employees who require access. The IT Team administers employees' access, which must be approved based on job role.

4.8.7 *Ad hoc* access to customer physical media pursuant to specific requests are administered by the IT Team with the approval of the employee's supervisor.

4.8.8 Everyone with access rights to an IPsoft Amelia LLC corporate office must sign a non-disclosure agreement.

4.8.10 Access cards and/or keys are not shared or loaned to others without authorization.

4.8.11 Access cards and/or keys that are no longer required are returned to the IT Team.

4.8.12 Cards are not reallocated to another individual, bypassing the return process.

4.8.13 IPsoft Amelia LLC employees are responsible for notifying the IT Team within 24 hours if their access cards and/or keys are lost, stolen, or compromised.

4.8.14 Cards and/or keys have no identifying information coded into them.

4.8.15 IPsoft Amelia LLC maintains an inventory of all customer physical media received by IPsoft Amelia LLC. IPsoft Amelia LLC imposes restrictions on handling Customer Data and has procedures for disposing of materials that contain Customer Data.

4.8.16 IPsoft Amelia LLC uses commercially reasonable processes to securely destroy customer physical media in accordance with the Customer Agreement.

4.9 Measures for ensuring events logging.

4.9.1 Event and system access logs are logged, monitored, and reviewed periodically.

4.9.2 User activity metrics and logs, configuration changes, deletions, and updates are written automatically to audit logs in operational systems.

4.9.3 User activity metrics are available to customers within the IPsoft Amelia LLC web application.

4.9.4 Audit logs maintain detailed information such as timestamp, IP address, specific action taken, requested metadata.

4.9.5 Certain log events on IPsoft Amelia LLC such as timestamps, IPs, login/logouts, and errors are available to authorized employees for security investigations.

4.9.6 Notifications and alerts are sent based on the rules configured in the monitoring systems to identify anomalies, suspicious network behavior, abnormal activities, and potential threats.

4.9.7 IPsoft Amelia LLC has a central Security Information and Event Management (SIEM) system and other product tools to monitor the security alerts generated by the IPsoft Amelia LLC Service.

4.10 Measures for ensuring system configuration, including default configuration.

4.10.1 IPsoft Amelia LLC has a Configuration Management Policy that allows IPsoft Amelia LLC to securely control assets, configurations, and changes throughout the software development lifecycle.

4.10.2 IPsoft Amelia LLC monitors changes to in-scope systems to ensure that changes follow the process and to mitigate the risk of undetected changes to the production environment. Changes are tracked in our change management platform.

4.11 Measures for internal security governance and IT Management.

4.11.1 IPsoft Amelia LLC maintains security documents describing its security measures and relevant procedures and responsibilities of its personnel. These include a suite of information security policies and procedures, security and privacy training documents, penetration and vulnerability scanning reports, and Service Organization Control ("SOC") 2 Type 2 (or comparable) reports.

4.11.2 IPsoft Amelia LLC has established an Information Security Management System in accordance with the International Organization for Standardization ("ISO") 27001:2013 standard. Information security-related business operations continue to be carried out in line with the ISO 27001:2013 standard.

4.11.3 The authority and responsibility for managing IPsoft Amelia LLC's information security program has been delegated to the Governance, Risk, and Compliance team, who is authorized by senior management to take actions necessary to establish, implement, and manage IPsoft Amelia LLC's information security program.

Measures for certification/assurance of processes and products.

4.11.4 IPsoft Amelia LLC's system of internal control requires annual independent third-party audits to test the operational effectiveness of its program and practices. Annual audits include SOC 2 Type 2 (Security, Privacy, Confidentiality & Availability) and ISO 27001.

4.11.5 In addition IPsoft Amelia LLC has engaged independent auditors to review its compliance status for both HIPAA and GDPR, attesting to our commitment to safeguard the confidentiality, integrity, and privacy of information stored and processed in our Service.

4.11.6 AWS has achieved: (A) SOC 1, 2, and 3; (B) ISO 27001, 27017, 27018, 27701, and 9001; (C) Cloud Security Alliance Security, Trust, Assurance and Risk Cloud Control Matrix v3.0.1; (D) FedRAMP; and (E) use FIPS 140-2 validated cryptographic modules, in addition to meeting compliance standards for many other legal, security, and privacy frameworks. Further information about AWS's security practices can be found at https://aws.amazon.com/compliance/data-center/controls/.

4.12 Measures for ensuring data minimization.

4.12.1 Customer Data collection by IPsoft Amelia LLC is limited to the purposes of processing (or the data that the Customer chooses to provide).

4.12.2 Security measures are in place to provide only the minimum amount of access necessary to perform the Service.

4.13 Measures for ensuring data quality.

4.13.1 IPsoft Amelia LLC has a process that allows individuals to exercise their privacy rights (including a right to amend and update information).

4.13.2 Software releases and updates/patches to IPsoft Amelia LLC production environments are tested for functionality and security, including any significant modifications, major enhancements, and new systems, prior to deployment.

4.14 Measures for ensuring limited data retention.

4.14.1 Customer Data is retained as per the contractual terms agreed with the Customer and as required by applicable privacy law.

4.14.2 After termination of a Subscription, Customer Data is deleted from the production environment within a commercially reasonable timeframe.

4.15 Measures for ensuring accountability.

4.15.1 Events and audit trails related to IPsoft Amelia LLC Service and system access are logged, monitored, and reviewed periodically.

4.15.2 IPsoft Amelia LLC adopts the Three Lines of Defense governance model for its system of internal control. This model is designed to ensure the effective and transparent management of compliance obligations and risks by making accountabilities clear across the organization.

4.16 Measures for allowing data portability and ensuring erasure.

4.16.1 Customers have the ability to export Customer Data to CSV, PDF, and ZIP formats via the IPsoft Amelia LLC web application.

4.16.2 IPsoft Amelia LLC has a process that allows individuals to exercise their privacy rights under applicable privacy law.

ANNEX C Standard Contractual Clauses 2021 (Module Two)

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);

(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

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 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 [(4)] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 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.[(8)] 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.

(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.

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[12];

(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

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 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

MODULE TWO: Transfer controller to processor

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 the Netherlands (specify Member State).

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 the Netherlands (specify Member State).

(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.

.

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

[4] 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.

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

[12] 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.

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES 2021 (MODULE TWO)

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or *contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.*

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES 2021 (MODULE TWO)

- **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

Defined terms used in this Annex I shall have the meaning given to them in the Agreement (including the DPA).

Data exporter(s): Name and address: The Customer, as defined in the Agreement Contact person's name, position and contact details: Name (full): […] Position: […] Address: […] Email: […] Phone: […] Activities relevant to the data transferred under these Clauses: The data exporter provides personal data to the data importer to the extend necessary for the data importer to provide the Service. Details regarding the processing can be found in the description of transfers below. Signature and date: […] Name of the signatory: Position of the signatory: Role: controller	**Data importer(s):** Name and address: Amelia US LLC, located at 17 State Street, 14th Floor, New York, New York 10004 USA Contact person's name, position and contact details: Name (full): Jeffrey Neu Position: Chief Legal Officer Address: 17 State Street, 14th Floor, New York, New York 10004 USA Email: Jeffrey.neu at ipsoft.com Phone: +1-212-708-5441 Activities relevant to the data transferred under these Clauses: The data importer processes the personal data as necessary to provide the Service. Details regarding the processing can be found in the description of transfers below. Signature and date: […] Name of the signatory: Jeffrey Neu Position of the signatory: Chief Legal Officer Role: processor
[…] PERMITTED AFFILIATES WHICH ARE ALSO DATA EXPORTERS NEED TO BE LISTED HERE AS WELL	

- **DESCRIPTION OF TRANSFERS**

MODULE TWO: Transfer controller to processor

- **Categories of data subjects whose personal data is transferred:** Please see Annex A of the DPA, which describes the data subjects.
- **Categories of personal data transferred:** Please see Annex A of the DPA, which describes the categories of data.
- **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:** The parties do not anticipate the transfer of sensitive data.
- **The frequency of the transfer** *(e.g. whether the data is transferred on a one-off or continuous basis)***:** The data is transferred on a continuous basis.
- **Nature of the processing:** The data importer will process personal data as necessary to provide the Services pursuant to the Agreement, as further specified in the applicable Order Form, and as further instructed by the data exporter.
- **Purposes of the data transfer and further processing:** The data importer shall process personal data as necessary to provide the Products/Services to data exporter in accordance with the Agreement.
- **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:** Subject to the "Deletion or Return of Personal Data" section of this DPA, the data importer will retain personal data for the duration of the Agreement, unless otherwise agreed in writings or as required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: For details see Annex A of this DPA. For sub-processors see Annex F of this DPA.

- **COMPETENT SUPERVISORY AUTHORITY**

MODULE TWO: Transfer controller to processor

The competent supervisory authority depends on the circumstances by which Regulation (EU) 2016/679 is applicable (cf. Clause 13):

- Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as 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 shall act as competent supervisory authority.

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES 2021 (MODULE TWO)

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

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Please see Annex B of the DPA, which describes the technical and organisational security measures implemented by IPsoft / Amelia.

ANNEX III TO THE STANDARD CONTRACTUAL CLAUSES 2021 (MODULE TWO)

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE: This Annex must be completed for Module Two, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

This Annex III is not applicable since Clause 9(a), Option 1 has not been chosen.

ANNEX D Standard Contractual Clauses 2021 (Module Three)

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);

(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

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 THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter(5).

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[6] (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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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 THREE: Transfer processor to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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.(9) 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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 THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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.

MODULE THREE: Transfer processor 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 THREE: Transfer processor 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 THREE: Transfer processor 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 THREE: Transfer processor 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:

(iv) 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;

(v) 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[12];

(vi) 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

MODULE THREE: Transfer processor to processor

15.3 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.

15.4 Review of legality and data minimisation

(d) 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).

(e) 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.

(f) 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

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

(g) 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).

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

(iv) 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;

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

(vi) 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.

(i) 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.

(j) 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 THREE: Transfer processor to processor

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 the Netherlands (specify Member State).

Clause 18

Choice of forum and jurisdiction

MODULE THREE: Transfer processor to processor

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

(f) The Parties agree that those shall be the courts of the Netherlands (specify Member State).

(g) 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.

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

.

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

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) 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 purposes of these Clauses.

[7] This includes whether the transfer and further processing 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 or offences.

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

[12] 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.

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES 2021 (MODULE THREE)

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES 2021 (MODULE THREE)

A. LIST OF PARTIES

MODULE THREE: Transfer processor to processor

Defined terms used in this Annex I shall have the meaning given to them in the Agreement (including the DPA).

Data exporter(s): Name and address: The Customer, as defined in the Agreement Contact person's name, position and contact details: Name (full): […] Position: […] Address: […] Email: […] Phone: […] Activities relevant to the data transferred under these Clauses: The data exporter provides personal data to the data importer to the extend necessary for the data importer to provide the Service. Details regarding the processing can be found in the description of transfers below. Signature and date: […] Name of the signatory: Position of the signatory: Role: processor	**Data importer(s):** Name and address: Amelia US LLC, located at 17 State Street, 14th Floor, New York, New York 10004 USA Contact person's name, position and contact details: Name (full): Jeffrey Neu Position: Chief Legal Officer Address: 17 State Street, 14th Floor, New York, New York 10004 USA Email: Jeffrey.neu at ipsoft.com Phone: +1-212-708-5441 Activities relevant to the data transferred under these Clauses: The data importer processes the personal data as necessary to provide the Service. Details regarding the processing can be found in the description of transfers below. Signature and date: […] Name of the signatory: Jeffrey Neu Position of the signatory: Chief Legal Officer Role: (sub)-processor
[…]Please note that Permitted Affiliates (which also are data exporters) need to be listed as well	

B. DESCRIPTION OF TRANSFERS

MODULE THREE: Transfer processor to processor

- **Categories of data subjects whose personal data is transferred:** Please see Annex A of the DPA, which describes the data subjects.
- **Categories of personal data transferred:** Please see Annex A of the DPA, which describes the categories of data.
- **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:** The parties do not anticipate the transfer of sensitive data.
- **The frequency of the transfer** *(e.g. whether the data is transferred on a one-off or continuous basis)***:** The data is transferred on a continuous basis.
- **Nature of the processing:** The data importer will process personal data as necessary to provide the Services pursuant to the Agreement, as further specified in the applicable Order Form, and as further instructed by the data exporter.
- **Purposes of the data transfer and further processing:** The data importer shall process personal data as necessary to provide the Products/Services to data exporter in accordance with the Agreement.
- **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:** Subject to the “Deletion or Return of Personal Data” section of this DPA, the data importer will retain personal data for the duration of the Agreement, unless otherwise agreed in writings or as required by applicable law.
- **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:** For details see Annex A of this DPA. For sub-processors see Annex F of this DPA.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE THREE: Transfer processor to processor

The competent supervisory authority depends on the circumstances by which Regulation (EU) 2016/679 is applicable (cf. Clause 13):

- Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as 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 shall act as competent supervisory authority.

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES 2021 (MODULE THREE)

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

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Please see Annex B of the DPA, which describes the technical and organisational security measures implemented by IPsoft / Amelia.

ANNEX III TO THE STANDARD CONTRACTUAL CLAUSES 2021 (MODULE THREE)

LIST OF SUB-PROCESSORS

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: This Annex must be completed for Module Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

This Annex III is not applicable since Clause 9(a), Option 1 has not been chosen.

ANNEX E Standard Contractual Clauses 2010

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

The Customer, as defined in the Agreement (the "data exporter") [...] Please note that Permitted Affiliates (which also are data exporters) need to be listed as well.
And

Amelia US LLC, located at 17 State Street, 14th Floor, New York, New York 10004 USA (the "data importer")

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

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

Clause 1. **Definitions**

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2. **Details of the transfer**

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

Clause 3. **Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6.1 and (2), Clause 7, Clause 8.2, and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data

subject so expressly wishes and if permitted by national law.

Clause 4. **Obligations of the data exporter**

The data exporter agrees and warrants:

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

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

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

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

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

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

g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

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

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

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

Clause 5. **Obligations of the data importer**

The data importer agrees and warrants:

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

b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

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

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

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

   ii) any accidental or unauthorised access; and

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

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

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

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

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

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

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

Clause 6. **Liability**

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

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

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

Clause 7. **Mediation and jurisdiction**

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

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

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

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

Clause 8. **Cooperation with supervisory authorities**

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

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is

subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

***Clause 9.* Governing law**

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

***Clause 10.* Variation of the contract**

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

***Clause 11.* Subprocessing**

a) The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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

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

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

***Clause 12.* Obligation after the termination of personal data-processing services**

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

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

On behalf of the data exporter: Name (full): Position: Address: Other information required for binding: Signature:	**On behalf of the data importer:** Name (full): Jeffrey Neu Position: Chief Legal Officer Address: 17 State Street, 14th Floor, New York, New York 10004 USA Other information: Signature:

Appendix 1 to the Standard Contractual Clauses 2010

This Appendix forms part of the Standard Contractual Clauses 2010 (the 'Clauses').

Defined terms used in this Appendix 1 shall have the meaning given to them in the Agreement (including the DPA).

- **Data exporter:** The data exporter is the legal entity specified as "Customer" in the DPA.
- **Data importer:** The data importer is Amelia US LLC.
- **Data subjects:** Please see Annex A of the DPA, which describes the data subjects.
- **Categories of data:** Please see Annex A of the DPA, which describes the categories of data.
- **Special categories of data (if appropriate):** The parties do not anticipate the transfer of special categories of data.
- **Purposes of Processing:** Amelia US LLC shall process personal data as necessary to provide the Products/Services to data exporter in accordance with the Agreement.
- **Processing operations:** Please see Annex A of the DPA, which describes the processing operations.

DATA EXPORTER

Name:	Authorized Signature:

DATA IMPORTER

Name: Jeffrey Neu, Chief Legal Officer	Authorized Signature:

Appendix 2 to the Standard Contractual Clauses 2010

This Appendix forms part of the Standard Contractual Clauses 2010 (the 'Clauses').

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5.2(c) (or document/legislation attached):

Please see Annex B of the DPA, which describes the technical and organisational security measures implemented by IPsoft / Amelia.

DATA EXPORTER

Name: Authorized Signature:

DATA IMPORTER

Name: Jeffrey Neu, Chief Legal Officer Authorized Signature:

Appendix 3 to the Standard Contractual Clauses 2010

This Appendix forms part of the Standard Contractual Clauses 2010 (the 'Clauses'). This Appendix sets out the parties' interpretation of their respective obligations under specific terms of the Clauses. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

For the purposes of this Appendix, "DPA" means the Data Processing Agreement in place between Customer and IPsoft / Amelia and to which these Clauses are incorporated, and "Agreement" shall have the meaning given to it in the DPA.

Clause 4(h) and 8: Disclosure of these Clauses

a) Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clauses 5(a) and 5(b): Suspension of data transfers and termination

a) The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

b) The parties acknowledge that if data importer cannot provide such compliance in accordance with Clause 5(a) and Clause 5(b) for whatever reason, the data importer agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract the affected parts of the Services in accordance with the terms of the Agreement.

c) If the data exporter intends to suspend the transfer of personal data and/or terminate the affected parts of the Services, it shall endeavor to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").

d) If required, the parties shall reasonably cooperate with each other during the Cure Period to agree what additional safeguards or other measures, if any, may be reasonably required to ensure the data importer's compliance with the Clauses and applicable data protection law.

e) If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend and/or terminate the affected part of the Services in accordance with the provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by the data exporter prior to suspension or termination). The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit

a) Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in the 'Demonstration of Compliance' section of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

a) The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

b) The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

c) Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably requires in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

a) Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

a) The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 (*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*), the data exporter may provide a general consent to onward subprocessing by the data importer.

b) Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer’s compliance with the requirements set out in the 'Notification and Objection to New Sub-Processors' section of the DPA.

Clause 12: Obligation after the termination of personal data-processing services

a) Data importer agrees that the data exporter will fulfil its obligation to return or destroy all the personal data on the termination of the provision of data-processing services by complying with the 'Deletion or Return of Personal Data' section of the DPA.

ANNEX F List of Sub-Processors

Sub-Processor	Subject Matter & Nature	Location
Amazon Web Services Inc./Amazon Web Services EMEA SARL Hosting*	Hosting & Infrastructure	United States, Luxembourg
Google Cloud Services*	Hosting & Infrastructure	United States, Republic of Ireland, Singapore
Microsoft Azure*	Hosting & Infrastructure	United States
IPsoft Incorporated**	Services & Support	United States, 17 State Street, New York, NY
Amelia Australia Pty. Ltd.	Services & Support	Lvl 36, Gateway, 1 Macquarie Place, Sydney, NSW 2000, Australia
Amelia (IPsoft) Canada Inc.	Services & Support	100 King Street West, Suite 5710, Toronto, Ontario, M5X 1C7 Canada
IPsoft EU Holding B.V.**	Services & Support	Weesperplein 4A, 1018XA Amsterdam, The Netherlands
IPsoft France SARL	Services & Support	9, Rue du Quatre Septembre Paris, 75002, France
IPsoft Global Services Pvt. Ltd.	Services & Support	5th Floor, Voyager Building, Whitefield Road, Bangalore, 560066, Republic of India
Amelia Japan K.K.	Services & Support	Ginza Six 13F, 6-10-1 Ginza, Chuo-ku, Tokyo, 104-0061, Japan
IPsoft Peru S.A.C.	Services & Support	Av. Victor Andres Belaunde 280 Int. 301, San Isidro, Lima , 051127, Peru
IPsoft Slovakia s.r.o.	Services & Support	Palisady 32, Bratislava 81106, Slovakia
IPsoft Spain S.L.U.	Services & Support	Paseo da la Castellana, 43 Madrid, 28046, Spain
Amelia (IPsoft UK) Ltd.	Services & Support	The Leadenhall Building , 122 Leadenhall Street, London EC3V 4AB, United Kingdom (England)
Amelia NL B.V.**	Services & Support	Weesperplein 4A, 1018XA Amsterdam, The Netherlands

Amelia Global Services Pvt. Ltd.	Services & Support	5th Floor, Voyager Building, Whitefield Road, Bangalore, 560066, Republic of India
Amelia Sweden A.B.	Services & Support	Drottninggatan 95A, Stockholm, 113 60 Sweden
Amelia US LLC**	Services & Support	United States, 17 State Street, New York, NY
IPsoft GmbH	Services & Support	Taunusanlage 8, 60329, Frankfurt, Germany

* Providers used for hosting and infrastructure, where IPsoft / Amelia is providing SaaS or similar services. Additionally, Google and Microsoft may be used to provide certain translation services, including text-to-speech and speech-to-text.** The IPsoft/Amelia entity which is Processor under the DPA consequently shall not be considered a Sub-Processor. *** Subject to the “Deletion or Return of Personal Data” section of this DPA, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writings or as required by applicable law.