DATA PROCESSING AGREEMENT

This 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 (also referred to in this DPA as the "Agreement") between you ("Customer") and the applicable Amelia legal entity ("Amelia" or "us").

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: https://amelia.ai/legal/dpa/. 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.

1. DEFINITIONS

"**Affiliate**" means an entity that controls, is controlled by or is under common control with the applicable party. For purposes of this definition, "control" means ownership of more than fifty (50%) percent of the voting stock or other ownership interest in an entity.

"**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 the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act and applicable implementing regulations ("**CCPA**") and European Data Protection Laws; in each case as amended, repealed, consolidated or replaced from time to time.

"**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); (iii) in respect of the United Kingdom, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) and any applicable national legislation that replaces or converts in domestic law the GDPR including The Data Protection Act 2018, including any guidance and amendments thereof or any other law relating to data and privacy as a consequence of the UK leaving the European Union; and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance and as revised as of 25 September 2020 ("**Swiss Data Protection Law**"); in each case, as may be amended, superseded or replaced.

"**IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses Version B1.0, in force 21 March 2022, as published, amended, superseded or replaced by the UK Information Commissioner's Office.

"**Instructions**" or "**instructions**" means the written, documented instructions issued by a Controller to a Processor or from a Processor to a Sub-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). Instructions include the rights and obligations with regard to processing of personal data included in the written terms of any agreement and this DPA.

"**Permitted Affiliates**" means any of your Affiliates that (i) are permitted to use the 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**" or "**personal data**" means personal data, personal information, and personally identifiable information as those terms are defined under Data Protection Laws, or other information relating to an identified or identifiable individual which is given similar protection under 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 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.

"**Processing**" or "**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.

"**Services**" shall have the meaning set forth in the Agreement (or applicable order), or in absence of a defined term in the Agreement, "Services" shall mean the products and services provided to Customer under the Agreement.

"**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 as may be amended, superseded, or replaced.

"**Sub-Processor**" means any processor of a Processor. Amelia's Sub-Processors may include third parties or our Affiliates but will exclude any Amelia employee or consultant.

The terms "**Controller**" (which includes "**Business**" as defined in the CCPA), "**Data Subject**" (which includes "**Consumer**" as defined in U.S. Privacy Laws), "**Processor**" (which includes "**Service Provider**" as defined in the CCPA) are defined as in respective Data Protection Laws.

2. CUSTOMER RESPONSIBILITIES

2.1 **Compliance with Laws**. Within the scope of the Agreement and 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 Personal 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 2.1 or applicable Data Protection Laws.

2.2 **Controller Instructions**. The parties agree that the Agreement (including this DPA), together with your use of the 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.

3. AMELIA'S GENERAL OBLIGATIONS

3.1 **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. 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 promptly notify you of that legal requirement to the extent permitted by the applicable law. 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 We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

3.2 **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.

3.3 **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.

3.4 **Personal Data Breaches**. We will notify you without undue delay and no later than within 72 hours 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.

3.5 **Deletion or Return of Personal Data**. We will delete or return all Personal Data 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 Personal Data, or to Personal 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 Rights Portal (https://app.onetrust.com/app/#/webform/9282f952-0743-4bcd-bd2c-9e6eba16424b) or by contacting your Amelia representative.

4. DATA SUBJECT REQUESTS

4.1 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").

4.2 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 reasonable costs arising from this assistance.

4.3 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.

5. SUB-PROCESSORS

5.1 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 C to this DPA.

5.2 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.

5.3 We will notify you of any material changes to our Sub-processors by updating Annex C, providing such update to you, and giving you 30 days to object to such changes. 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 and due to us prior to suspension or termination).

6. DATA TRANSFERS.

6.1 **General**. 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 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.

7 AUDITS

7.1 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. 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 that portions of the Services are hosted by our data center partners who maintain independently validated security programs (such as SOC 2 and ISO 27001) and that our systems are regularly tested by independent third-party penetration testing firms. Upon written request, we will supply (on a confidential basis) a summary copy of such 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.

8 ADDITIONAL TERMS

8.1 **European Union**. Where you are the Controller and Amelia the Processor of Personal Data under European Data Protection Laws, the Standard Contractual Clauses (Module 2) are incorporated by this reference and form an essential part of the DPA. Where you are the Processor and Amelia the Sub-Processor of Personal Data under European Data Protection Laws, the Standard Contractual Clauses (Module 3) are incorporated by this reference and form an essential part of the DPA. In all cases:

- Clause 7 (the optional docking clause) is included;
- Under Clause 9 (Use of sub-processors), the parties select Option 2 (General written authorization);
- Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply;
- Under Clause 17 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of the Netherlands;
- Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of the Netherlands;
- Annexes I-III of the EU SCCs are set forth in Annexes A-C, respectively, of the DPA; and
- By entering into this DPA, the parties are deemed to be signing the EU SCCs and its applicable annexes.

8.2 **United Kingdom**. With respect to Personal Data transferred from the UK for which UK law (and not the law in any European Economic Area jurisdiction) governs the nature of the transfer, the IDTA is incorporated by this reference and forms an essential part of the DPA. In addition:

- In Table 1 of the IDTA: (1) the Parties' details shall be the parties and their affiliates, as applicable, and (2) the Key Contact shall be the contacts set forth in Annex A of the DPA;
- In Table 2 of the IDTA: the Approved EU SCCs shall be those referenced in Section 8.1 of the DPA;
- In Table 3 of the IDTA: Annex 1A, 1B, II, and III shall be as set forth in Annexes A-C of the DPA;
- In Table 4 of the IDTA: either Party may end this DPA; and
- By entering into this DPA, the Parties are deemed to be signing the IDTA.

8.3 **Switzerland**. With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the nature of the transfer, references to the GDPR in Clause 4 of the EU SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner. Any Standard Contractual Clauses are deemed to be edited in all other ways necessary to accommodate the application of Swiss Data Protection Law.

8.4 **California**. When processing Personal Data subject to CCPA, the parties acknowledge and agree that: (i) you are a Business, (ii) we are a Service Provider, (iii) we will only process such personal data strictly for the purpose of performing the Services or as otherwise expressly permitted under the Agreement or as otherwise permitted by law, and (iii) we will not "Sell" (as that term is defined under CCPA) such Personal Data.

The parties have caused this DPA to be executed by the signature of their duly authorized representatives below.

For Amelia:	**For Customer:**
By: _____	By: _____
Name: _____	Name: _____

Title: _____ Title: _____

Date: _____ Date: _____

ANNEX A
DETAILS OF PROCESSING

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.

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.

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:

- Your users and other end users including your employees, contractors, collaborators, customers, prospects, suppliers, and subcontractors.
- Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to your end users.
- Your users who are authorized by you to use the Services.

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:

- Names, Titles, Positions, and Employer Information
- Contact Information, such as email addresses, work addresses, and other physical location data,
- Connection data related to the access to the Services, except to the extent that such data is anonymized or pseudonymized,
- Conversation data related to the usage of the Services, except to the extent that such data is anonymized or pseudonymized,
- Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Services.

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

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

- Storage and other Processing necessary to provide, maintain, and improve the Services provided to you; and/or
- Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

ANNEX B

TECHNICAL AND ORGANIZATIONAL MEASURES

1 Measures of pseudonymization and encryption of personal data.

- Amelia requires full-disk hard drive encryption using AES-256 for all employee computers, and uses role-based access control, multi-factor authentication, and account management procedures to control access to Customer Data.
- Amelia encrypts data in transit and at rest using hybrid encryption techniques that align with NIST Special Publication 800-53.
- Customer Data at rest is encrypted using the AES-256 algorithm.
- Amelia uses TLS version 1.2 or higher to protect HTTPS communications.
- For email security, Amelia uses opportunistic TLS encryption (OE).
- Customer Data that is hosted with AWS is encrypted at rest as described in AWS's documentation available at https://aws.amazon.com/compliance/data-center/controls/.
- AWS log-in credentials and private keys generated by the Service are for Amelia's internal use only.
- Encryption keys are rotated.

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

- Amelia maintains a record of personnel authorized to access systems that contain Customer Data.
- Privileged access requires a formal account management and access control procedure that requires review and approval from a line manager or other executives.
- Amelia 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.
- Amelia's personnel are legally obligated to maintain the confidentiality of Customer Data and this obligation continues after their employment or service ends.
- Employees complete mandatory training annually, which covers data privacy and governance, data protection, confidentiality, social engineering, password policies, and information security.
- Amelia requires difficult-to-guess passwords for all employees and follows NIST best practices.
- Amelia web application account passwords are hashed when stored.
- Amelia web application sessions expire after 30 minutes of inactivity.
- The Amelia web application retains session locks until the session user reestablishes access Amelia identification and authorization procedures.

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.

- Amelia maintains geographically distributed data centers using AWS cloud hosting infrastructure.
- Amelia's information systems use security logs and alerting.
- Amelia's incident reporting and response procedure aligns with NIST SP 800-61 guidance on handling incidents, including steps for breach notification.
- All incidents are logged in an incident tracking system that is subject to annual audit.
- Amelia has a business continuity and disaster recovery plan that incorporates input from periodic risk assessments, vulnerability scanning, and threat analysis.
- Amelia 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 Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.

- Amelia conducts regular risk assessments and monitors the effectiveness of its safeguards, controls, and systems, through regular vulnerability scans, penetration testing, and intrusion detection.
- Amelia's vulnerability management program includes an independent testing team to perform vulnerability scanning to assess its internal and external network environments against emerging security threats.
- Amelia implements server protection on the production environment and endpoint protection on laptop/desktop endpoints, including continuously updated antivirus software.
- The servers that host the Amelia Service are scanned for viruses and malware on a weekly basis.
- The Amelia web application, network segmentation, and interconnections are protected by firewalls.
- Amelia services operate in separate, virtual networks that are isolated from other external traffic.
- Amelia's corporate equipment is protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access.
- Sub-processors undergo onboarding due diligence to ensure compliance with security and privacy requirements, laws, and regulations. To the extent applicable, sub-processors are required to sign a Data Processing Addendum that includes compliance with data protection laws and our customer agreements.

5 Measures for user identification and authorization.

- Amelia uses commercially reasonable practices to identify and authenticate users accessing its information systems and which are designed to maintain the confidentiality and integrity of account credentials when they are assigned and distributed and during storage.
- Customers manage their own password complexity and SSO/SAML 2.0 requirements.

6 Measures for the protection of Customer Data during transmission.

- Customer Data is encrypted in transit.
- All communications between the Customer and Amelia, as well as all third-party applications, take place over a secure HTTPS connection using TLS 1.2 or higher protocol.
- The Amelia production environments include logical and physical separation of components using networking and software defined networking technologies where appropriate. Production, testing, and staging environments are logically separated.
- All connections between Amelia internal networks and the Internet or any other publicly accessible computer network include an approved firewall or related access control system.

7 Measures for the protection of Customer Data during storage.

- Customer Data is hosted by AWS. Amelia maintains complete administrative control over its virtual servers.
- AWS Key Management System is used to encrypt data in our cloud infrastructure using FIPS 140-2 validated hardware security modules to protect keys from unauthorized access.
- Customer Data within Amelia's multi-tenant environments is logically segregated and attempts to access Customer Data outside allowed domain boundaries are prevented and logged.
- The Amelia web application runs antivirus scans regularly to detect malicious files present in the production environment and all personal data access is logged.
- Customer Data is protected during storage by AWS endpoint protection, firewalls, and antivirus.

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

- Physical access to data hosting facilities is documented and managed by AWS.
- Amelia limits access to its corporate offices to identified authorized individuals who require access for the performance of their job function and authorized, escorted visitors.
- Amelia uses commercially reasonable systems and measures to protect against loss of data due to power

supply failure or disruptions to Amelia's corporate office.

- 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.
- Amelia maintains an inventory of all customer physical media received by Amelia. Amelia imposes restrictions on handling Customer Data and has procedures for disposing of materials that contain Customer Data.
- Amelia uses commercially reasonable processes to securely destroy customer physical media in accordance with the Customer Agreement.
- Everyone with access rights to an Amelia corporate office must sign a non-disclosure agreement.
- Access cards and/or keys are not shared.
- Access cards and/or keys that are no longer required are returned to the IT Team or disabled.
- Amelia employees are responsible for notifying the IT Team within 24 hours if their access cards and/or keys are lost, stolen, or compromised.
- Cards and/or keys have no identifying information coded into them.

9 Measures for ensuring events logging.

- Event and system access logs are monitored and reviewed periodically.
- User activity metrics and logs, configuration changes, deletions, and updates are written automatically to audit logs in operational systems.
- User activity metrics are available to customers within the Amelia web application.
- Audit logs maintain timestamp, IP address, specific action taken, and certain requested metadata.
- Certain log events on Amelia such as timestamps, IPs, login/logouts, and errors are available to authorized employees for security investigations.
- 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.
- Amelia has a central security information and event management system and other product tools to monitor the security alerts generated by the Amelia Service.

10 Measures for ensuring system configuration, including default configuration.

- Amelia has a configuration management policy to securely control assets, configurations, and changes throughout the software development lifecycle.
- Amelia monitors and logs all changes to in-scope systems to ensure that changes follow the process and to mitigate the risk of undetected changes to the production environment.

11 Measures for internal security governance and IT Management.

- Amelia maintains appropriate documentation describing its security measures and relevant procedures and responsibilities of its personnel.
- Amelia has established an Information Security Management System in accordance with ISO 27001:2013.
- Managing Amelia's information security program is the responsibility of the Governance, Risk, and Compliance team who is authorized by senior management to take all reasonable actions necessary to establish, implement, and manage Amelia's information security program.

12 Measures for certification/assurance of processes and products.

- Amelia'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.
- Amelia uses independent auditors to review its compliance status for HIPAA and GDPR, attesting to our

commitment to safeguard the confidentiality, integrity, and privacy of information stored and processed in our Service.
- AWS certifies or attests to: (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) FIPS 140-2. Further information can be found at https://aws.amazon.com/compliance/data-center/controls/.

13 Measures for ensuring data minimization.

- Amelia only collects data that the Customer chooses to provide as part of receiving the Services.
- Amelia returns or destroys Customer Data at the Customer's request in accordance with the Agreement.

14 Measures for ensuring data quality.

- Amelia will assist customers acting on a data subject access request to amend or correct information.
- Software releases and updates/patches to Amelia production environments are tested for functionality and security, including any significant modifications, major enhancements, and new systems, prior to deployment.

15 Measures for ensuring limited data retention.

- Customer Data is retained as per the contractual terms agreed with the Customer and as required by applicable privacy law.
- After termination of a Subscription, Customer Data is deleted from the production environment within a commercially reasonable timeframe.

16 Measures for ensuring accountability.

- Events and audit trails related to Amelia Service and system access are logged and regularly reviewed.
- Amelia adopts the Three Lines of Defense governance model for its system of internal control for transparent management of compliance obligations and risks.

17 Measures for allowing data portability and ensuring erasure.

- Customers can export Customer Data at any time to .csv, .pdf, and .zip formats.
- Amelia allows individuals to exercise their privacy rights under applicable privacy law.

ANNEX C

SUB-PROCESSOR LIST

Sub-Processor	Nature of processing	Location of Processing
Amazon Web Services Inc./Amazon Web Services EMEA SARL Hosting	Hosting, infrastructure	United States, Luxembourg
Google Cloud Services	Hosting, infrastructure, and services	United States, Republic of Ireland, Singapore
Microsoft Azure	Hosting, infrastructure, and services	United States
Amelia Australia Pty. Ltd.	Services, support	Australia
Amelia (IPsoft) Canada Inc.	Services, support	Canada
IPsoft France SARL	Services, support	France
IPsoft Peru S.A.C.	Services, support	Peru
Amelia Artificial Intelligence SL	Services, support	Spain
Amelia Sweden AB	Services, support	Sweden
Amelia GmbH	Services, support	Germany
Amelia EU Holding B.V.	Services, support	The Netherlands
Amelia NL B.V.	Services, support	The Netherlands
Amelia Global Services Pvt. Ltd.	Services, support	Republic of India
Amelia US LLC	Services, support	United States
IPsoft Government Solutions LLC	Services, support	United States