EQUAL TIME

Data Processing Agreement in accordance with Art. 28 GDPR

This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Principal Agreement") between _____ (the "the "Controller") and Equalicert Inc (the "Processor") (together as the "Parties")

Preamble

The Controller has selected the Processor to act as a service provider in accordance with Art. 28 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "**GDPR**").

This Data Processing Agreement, including all Annexes (hereinafter referred to collectively as the "**Agreement**"), specifies the data protection obligations of the parties from the underlying Principal Agreement, the Service Level Agreement and/or the order descriptions (hereinafter referred to collectively as the "**Principal Agreement**").

The Processor guarantees the Controller that it will fulfill the Principal Agreement and this Agreement in accordance with the following terms:

Sect.1 Scope and definitions

(1) The following provisions shall apply to all services of data processing provided by the Processor on behalf of the Controller under Art. 28 GDPR, which the Processor performs on the basis of the Principal Agreement.

(2) If this Agreement uses the term "data processing" or "processing" of data, this shall be generally understood to mean the use of personal data. Data processing or the processing of data shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(3) Reference is made to further definitions set forth in Art. 4 GDPR.

Sect.2 Subject matter and duration of the data processing

(1) The Processor shall process personal data on behalf and in accordance with the instructions of the Controller.

(2) The data processing shall involve carrying out the training of employees within the scope agreed with the Controller as agreed upon in the Principal Agreement.

(3) The duration of this Agreement corresponds to the duration of the Principal Agreement.

Sect.3 Nature and purpose of the data processing

The nature and purpose of the processing of personal data by the Processor is specified in the Principal Agreement. The Principal Agreement includes the following activities and purposes:

The person responsible shall provide the processor with selected data in accordance with § 5 of this agreement. The contract Processor uses this customer data to provide and document the training service as described in the main contract.

Sect.4 Categories of data subjects

The categories of individuals affected by the processing of personal data under this Agreement (“data subjects”) include:

Employees who have been authorized by the Controller to use the service, provided they are natural persons.

Sect.5 Types of personal data

The following types of personal data shall be processed under this Agreement:

- Master data of the employees as agreed with the Controller, usually first name, surname, and e-mail address. This may also include employee preferred pronouns or gender, team, level of

seniority in the company or other demographic data that the Controller wishes to share with Equal Time.

- Time, title and amount of speaking time in meetings where Equal Time was used

Sect.6 Rights and duties of the Controller

(1) The Controller is solely responsible for assessing the lawfulness of the data processing and for safeguarding the rights of data subjects, and is hence a controller within the meaning of Art. 4 (7) GDPR.

(2) The Controller is entitled to issue instructions concerning the nature, scale and method of data processing. Upon request by the Processor, the Controller shall confirm verbal instructions immediately in writing or in text form (e.g. by email) to the Processor.

(3) Insofar as the Controller deems it necessary, persons authorized to issue instructions may be appointed. The Processor shall be notified of such in writing or in text form. In the event that the persons authorized to issue instructions change, the Controller shall notify the Processor of this change in writing or in text form, naming the new person in each case.

(4) The Controller shall notify the Processor immediately of any errors or irregularities detected in relation to the processing of personal data by the Processor.

Sect.7 Duties of the Processor

(1) Data processing

- The Processor shall process personal data exclusively in accordance with this Agreement and/or the underlying Principal Agreement and in accordance with the Controller's instructions.

(2) Data subjects' rights

- The Processor shall, within its capabilities, assist the Controller in complying with the rights of data subjects, particularly with respect to rectification, restriction of processing, deletion of data, notification and information. If the Processor processes the personal data specified under Sect. 5 of this Agreement on behalf of the Controller and these data are the subject of a data portability request under Art. 20 GDPR, the Processor shall,

upon request, make the dataset in question available to the Controller within a reasonably set time frame, in a structured, commonly used and machine-readable format.

- If so instructed by the Controller, the Processor shall rectify, delete or restrict the processing of personal data specified under Sect. 5 of this Agreement. The same applies if this Agreement stipulates the rectification, deletion or restriction of the processing of data.
- If a data subject contacts the Processor directly to have his or her personal data specified under Sect. 5 of this Agreement rectified, deleted or the processing restricted, the Processor shall forward this request to the Controller immediately upon receipt.

(3) Monitoring duties

- The Processor shall ensure, by means of appropriate controls, that the personal data processed on behalf of the Controller are processed solely in accordance with this Agreement and/or the Principal Agreement and/or the relevant instructions.

- The Processor shall organize its business and operations in such way that the data processed on behalf of the Controller are secured to the extent necessary in each case and protected from unauthorized access by third parties.

- The Processor confirms that it has appointed a Data Protection Officer in accordance with Art. 37 GDPR and, if applicable, in accordance with Sect. 38 FDPA, and that the Processor shall monitor compliance with data protection and security laws. For questions about data protection the Controller can be contacted via legal@equaltime.io

(4) Information duties

- The Processor shall inform the Controller immediately if, in its opinion, an instruction issued by the Controller violates legal regulations. In such cases, the Processor shall be entitled to suspend execution of the relevant instruction until it is confirmed or changed by the Controller.
- The Processor shall assist the Controller in complying with the obligations set out in Articles 32 to 36 GDPR taking into account the nature of processing and the information available to the Processor.

(5) Location of processing and Data Transfers

- You acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Subscription Service in accordance with the Agreement, and in particular that Personal Data may be transferred to and Processed by Equalicert, Inc. in the United States and to other jurisdictions where Equalicert Affiliates and Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

(6) Deletion of personal data after order completion

- After termination of the Principal Agreement, the Processor shall delete or return all the personal data processed on behalf of the Controller to the Controller within 18 months after the end of the provision of services relating to processing and delete existing copies, provided that the deletion of these data does not conflict with any statutory storage obligations of the Processor. The deletion in accordance with data protection and data security regulations must be documented and confirmed upon request to the Controller.

Sect. 8 Monitoring rights of the Controller

(1) The Controller shall be entitled, after prior notification in good time and during normal business hours, to carry out an inspection of compliance with the provisions on data protection and the contractual agreements to the extent required, either himself or through third parties, without disrupting the Processor's business operations or endangering the security measures for other Controller and at his own expense. Controls can also be carried out by accessing existing industry-standard certifications of the Processor, current attestations or reports from an independent body (such as auditors, external data protection officers or external data protection auditors) or self-assessments. The Processor shall offer the necessary support to carry out the checks.

(2) The Processor shall inform the Controller of the execution of inspection measures by the supervisory authority to the extent that such measures or requests may concern data processing operations carried out by the Processor on behalf of the Controller.

Sect.9 Subprocessing

(1) The Controller authorizes the Processor to make use of other processors in accordance with the following subsections in Sect. 9 of this Agreement. This authorization shall constitute a

general written authorization within the meaning of Art. 28 (2) GDPR.

(2) The Processor currently works with the subcontractors specified in **Annex 2** and the Controller hereby agrees to their appointment.

(3) The Processor shall be entitled to appoint or replace other processors. The Processor shall inform the Controller in advance of any intended change regarding the appointment or replacement of other processors. The Controller may object to an intended change.

(4) The objection to the intended change must be lodged with the Processor within 2 weeks after receipt of the information on the change. In the event of an objection, the Processor may, at his own discretion, either provide the service without the intended change or propose an alternative subcontractor and coordinate it with the Controller. Insofar as the provision of the service is unreasonable for the Processor without the intended modification - for example, due to the associated disproportionate costs for the Processor - or the agreement on an alternative subcontractor fails, the Controller and the Processor may terminate this Agreement as well as the Principal Agreement with a notice period of one month to the end of the month.

(5) A level of protection comparable to that of this Agreement must always be guaranteed when other processors are involved. The Processor is liable to the Controller for all acts and omissions of other processors it appoints.

Sect. 10 Confidentiality

(1) The Processor is obliged to maintain confidentiality when processing data for the Controller.

(2) In fulfilling its obligations under this Agreement, the Processor undertakes to employ only employees or other agents who are committed to confidentiality in the handling of personal data provided and who have been appropriately familiarized with the requirements of data protection. Upon request, the Processor shall provide the Controller with evidence of the confidentiality commitments.

(3) Insofar as the Controller is subject to other confidentiality provisions, it shall inform the Processor accordingly. The Processor shall oblige its employees to observe these confidentiality rules in accordance with the requirements of the Controller.

Sect. 11 Technical and organizational measures

(1) The technical and organizational measures described in **Annex 1** are agreed upon as appropriate. The Processor may update and amend these measures provided that the level of protection is not significantly reduced by such updates and/or changes.

(2) The Processor shall observe the principles of due and proper data processing in accordance with Art. 32 in conjunction with Art. 5 (1) GDPR. It guarantees the contractually agreed and legally prescribed data security measures. It will take all necessary measures to safeguard the data and the security of the processing, in particular taking into account the state of the art, as well as to reduce possible adverse consequences for the affected parties. Measures to be taken include, in particular, measures to protect the confidentiality, integrity, availability and resilience of systems and measures to ensure continuity of processing after incidents. In order to ensure an appropriate level of processing security at all times, the Processor will regularly evaluate the measures implemented and make any necessary adjustments.

Sect. 12 Liability/Indemnification

(1) The Controller shall indemnify the Processor against any and all claims for damages asserted against the Processor based on the Controller's culpable breach of its own obligations under this Agreement or under applicable data protection and security regulations.

Sect. 13 Miscellaneous

(1) In case of contradictions between the provisions contained in this Agreement and provisions contained in the Principal Agreement, the provisions of this Agreement shall prevail.

(2) Amendments and supplements to this Agreement shall be subject to the mutual consent of the contracting parties, with specific reference to the provisions of this Agreement to be amended. Verbal side agreements do not exist and shall also be excluded for any subsequent changes to this Agreement.

(3) This Agreement is exclusively subject to the laws of the state of Delaware in the United States of America.

(4) In the event that access to the data which the Controller has transmitted to the Processor for

data processing is jeopardized by third-party measures (measures taken by an insolvency administrator, seizure by revenue authorities, etc.), the Processor shall notify the Controller of such without undue delay.

Schedule of Annexes

Annex 1 Technical and organizational measures taken to ensure the security of processing

Annex 2 Subprocessors pursuant to Sect. 9 of this Data Processing Agreement

EQUAL TIME

Annex 1

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centers. Production servers and client-facing applications are logically and physically secured from our internal corporate information systems. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures

implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Code stored in our source code repositories is checked for best practices and identifiable software flaws using automated tooling.

Penetration testing: We maintain relationships with industry-recognized penetration testing service providers for penetration testing of both the Equalicert web application and internal corporate network infrastructure at least annually. The intent of these penetration tests is to identify security vulnerabilities and mitigate the risk and business impact they pose to the in-scope systems.

Bugs: We welcome disclosure of security flaws in an effort to widen the available opportunities to engage with the security community and improve the product defenses against sophisticated attacks.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” (JITA) requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Administrative or high risk access permissions are reviewed at least once every six months.

b) Transmission Control

In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces and for free on every customer site hosted on the Equalicert products. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and heating, ventilation and air conditioning (HVAC) services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.
Disaster Recovery Plans: We maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes. Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

EQUAL TIME

Annex 2

Please see this webpage for an up-to-date list of subprocessors:
https://equaltime.io/gdpr-subprocessors/
Email legal@equaltime.io if you would like to be notified about changes to our subprocessors.

EQUAL TIME

Signature Page

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Controller Company

Signature _____

Name: _____

Title: _____

Date Signed: _____

Processor Company

Signature _____

Name _____

Title _____

Date Signed _____