ZEIT

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is an agreement between ZEIT, Inc. ("ZEIT," "we," "us," or "our") and you or the entity you represent ("Customer", "you" or "your"). This DPA supplements the ZEIT Enterprise Services Order Form and Enterprise Terms and Conditions, as updated from time to time between Customer and ZEIT, or any other agreement between Customer and ZEIT governing Customer's use of the Services (collectively, "Services Agreement"). This DPA applies when any Customer Data processed by ZEIT is subject to the GDPR (as defined below).

1. Definitions. Unless otherwise defined in the Services Agreement, all capitalized terms used in this DPA will have the meanings given to them below or as set forth in the GDPR:

1.1. "ZEIT Network" means ZEIT's owned or utilized facilities, servers, networking equipment, and host software systems (e.g., virtual private clouds) that are within ZEIT's control and are used to provide the Services.

1.2. "ZEIT Security Standards" means the security standards attached to the Services Agreement, or if none are attached to the Services Agreement, attached to this DPA as Annex 1.

1.3. "Customer" means you or the entity you represent.

1.4. "Customer Data" means the "Personal Data" (as defined under GDPR) that is uploaded by Customer to the Services under Customer's ZEIT accounts.

1.5. "EEA" means the European Economic Area.

1.6. "Data Protection Legislation" means (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the European Directives 95/46 and 2002/58/EC (as amended by Directive 2009/136/EC) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them; (ii) all relevant Member State laws or regulations giving effect or corresponding with the GDPR; (iii) any implementing legislation or legislation having equivalent effect in the United Kingdom to the extent the United Kingdom is no longer a Member State; and (iv) any judicial or administrative interpretation of any of the above, any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant supervisory authority and binding under applicable law.

1.7. "Processing" has the meaning given to it under GDPR and "Process", "Processes" and "Processed" will be interpreted accordingly.

1.8. "Security Incident" means a breach of ZEIT's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

2. Data Processing. This DPA applies when Customer Data is Processed by ZEIT. ZEIT will act as a Processor to Customer who may act as "Controller" (as such term is defined by GDPR) or Processor with respect to Customer Data.

2.1. Customer Controls. The Services provide Customer with a number of controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Customer Data as described in the Documentation. Without prejudice to Section 6.1, Customer may use these controls to assist it in connection with its obligations under Data Protection Legislation, including its obligations related to responding to requests from Data Subjects.

2.2. Details of Data Processing.

a. Subject matter. The subject matter of the Processing under this DPA is Customer Data.

b. Duration. As between ZEIT and Customer, the duration of the Processing under this DPA is determined by Customer.

c. Purpose. The purpose of the Processing under this DPA is the provision of the Services initiated by Customer from time to time.

d. Nature of the Processing. Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.

e. Type of Customer Data. Customer Data uploaded to the Services under Customer's ZEIT accounts.

f. Categories of Data Subjects. Data Subjects may include Customer's customers, employees, suppliers and end-users.

2.3. Compliance with Laws. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including Data Protection Legislation.

2.4. Customer Obligations. Customer is solely responsible for (i) the accuracy, quality, and legality of the Customer Data provided to ZEIT by (or on behalf) of Customer, (ii) the means by which Customer acquires any such Customer Data, including establishing all required legal bases (and obtaining and recording consent where consent is required) for the Processing contemplated hereunder, (iii) informing Data Subjects of the Processing of their Personal Data by ZEIT (as applicable), and (iv) the instructions it provides to ZEIT regarding the Processing of Customer Data. Customer will not provide or make available to ZEIT any Customer Data in violation of the Services Agreement, this DPA or Data Protection Legislation, or that is otherwise inappropriate for the nature of the Services to be provided by ZEIT, and shall promptly notify ZEIT where Customer Data that is Processed by ZEIT must no longer be Processed by reason of a Data Subject's request for deletion or withdrawal of consent, or any other legally valid obligation under Data Protection Legislation that mandates the cessation of Processing by ZEIT. If Customer is itself a processor, Customer warrants to ZEIT that

Customer's instructions and actions with respect to such Personal Data, including its appointment of ZEIT as another Processor, have been authorized by the relevant Controller.

3. Customer Instructions. The parties agree that this DPA and the Services Agreement (including the provision of instructions via configuration tools such as the ZEIT Command Line Interface and APIs made available by ZEIT for the Services) constitute Customer's documented instructions regarding ZEIT's Processing of Customer Data ("Documented Instructions"). ZEIT will Process Customer Data only in accordance with Documented Instructions; provided, however, that such limitations will not apply with respect to ZEIT's (i) internal purposes of developing anonymized and aggregated usage and performance metrics for reporting or statistical purposes, (ii) security and fraud prevention, and/or (ii) compliance with ZEIT's legal and regulatory obligations. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between ZEIT and Customer, including agreement on any additional fees payable by Customer to ZEIT for carrying out such instructions. Customer is entitled to terminate this DPA and the Services Agreement if ZEIT declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA.

4. Confidentiality of Customer Data. ZEIT will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a government body (such as a subpoena or court order). If a government body sends ZEIT a demand for Customer Data, ZEIT will attempt to redirect the government body to request that data directly from Customer. As part of this effort, ZEIT may provide Customer's basic contact information to the government body. If compelled to disclose Customer Data to a government body, ZEIT will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless ZEIT is legally prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this Section 4 varies or modifies the Standard Contractual Clauses.

5. Confidentiality Obligations of ZEIT Personnel. ZEIT restricts its personnel from Processing Customer Data without authorization by ZEIT as described in the ZEIT Security Standards. ZEIT imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

6. Security of Data Processing.

6.1. ZEIT has implemented and will maintain appropriate technical and organizational measures for the ZEIT Network as described in this Section. In particular, ZEIT has implemented and will maintain the following technical and organizational measures:

- **a.** security of the ZEIT Network as set out in the ZEIT Security Standards;
- **b.** physical security of the facilities as set out in the ZEIT Security Standards;

c. measures to control access rights for ZEIT employees and contractors in relation to the ZEIT Network as set out in the ZEIT Security Standards; and

d. processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by ZEIT as described in the ZEIT Security Standards.

6.2. Customer may elect to implement technical and organizational measures in relation to Customer Data. Such technical and organizational measures include the following which may be obtained by Customer from ZEIT, or directly from a third party supplier:

a. pseudonymization and encryption to ensure an appropriate level of security;

b. measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are being operated by Customer;

c. measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

d. processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

7. Sub-processing.

7.1. Authorized Sub-processors. Customer agrees that ZEIT may use sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services. Customer consents to ZEIT's use of sub- processors as described in this Section. Except as set forth in this Section, or as Customer may otherwise authorize, ZEIT will not permit any sub-processor to carry out Processing activities on Customer Data on behalf of Customer.

7.2. Sub-processor Obligations. Where ZEIT authorizes any sub-processor as described in Section 7.1:

a. ZEIT will restrict sub-processor's access to Customer Data to what is necessary to maintain the Services or to provide the Services to Customer and any End Users in accordance with the Documentation and ZEIT will prohibit the sub-processor from accessing Customer Data for any other purpose; ZEIT will enter into a written agreement with the sub-processor and, to the extent that the sub-processor is performing the same Processing services that are being provided by ZEIT under this DPA, ZEIT will impose on the sub-processor the same contractual obligations that ZEIT has under this DPA; and

b. ZEIT will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processors that cause ZEIT to breach any of ZEIT's obligations under this DPA.

8. Data Subject Rights. Taking into account the nature of the Services, ZEIT offers Customer

certain controls as described in Sections 2.1 and 6.2 that Customer may elect to use to comply with its obligations towards Data Subjects. Should a Data Subject contact ZEIT with regard to correction or deletion of its Personal Data, ZEIT will use commercially reasonable efforts to forward such requests to Customer; *provided, however*, that Customer shall remain responsible for handling and responding to any Data Subject requests as required by Data Protection Legislation.

9. Optional Security. ZEIT makes available a number of security features and functionalities that Customer may elect to use. Customer is responsible for (a) implementing the measures described in Section 6.2, as appropriate, (b) properly configuring the Services, (c) using the controls available in connection with the Services (including the security controls) to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (e.g. backups and routine archiving of Customer Data), and (d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

10. Security Breach Notification.

10.1. Security Incident. ZEIT will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

10.2. ZEIT Assistance. To assist Customer in relation to any Personal Data breach notifications Customer is required to make under GDPR, ZEIT will include in the notification under section 10.1(a) such information about the Security Incident as ZEIT is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to ZEIT, and any restrictions on disclosing the information, such as confidentiality.

10.3. Unsuccessful Security Incidents. Customer agrees that:

a. An unsuccessful Security Incident will not be subject to this Section 10. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of ZEIT's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful login attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

b. ZEIT's obligation to report or respond to a Security Incident under this Section 10 is not and will not be construed as an acknowledgement by ZEIT of any fault or liability of ZEIT with respect to the Security Incident.

10.4. Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means ZEIT selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the ZEIT team console and secure transmission at all times.

11. Assistance and Audits.

11.1. Data Protection Impact Assessment. Taking into account the nature of the Processing and the information available to ZEIT, ZEIT will provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Customer does not otherwise have access to the relevant information. Customer will be responsible for any costs and expenses arising from any such assistance by ZEIT, unless prohibited by applicable law.

11.2. Prior Consultation. Taking into account the nature of the Processing and the information available to ZEIT, ZEIT will provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer will be responsible for any costs and expenses arising from any such assistance by ZEIT, unless prohibited by applicable law.

11.3. Inspection. Upon Customer's reasonable request, and no more than once per calendar year, ZEIT will make available for Customer's inspection and audit, copies of certifications, records or reports demonstrating ZEIT's compliance with this DPA. In the event that Customer reasonably determines that it must inspect ZEIT's premises or equipment for purposes of this DPA, then no more than once per calendar year, any audits described in this Section 11 will be conducted, at Customer's expense, through an independent third-party auditor ("Independent Auditor") designated by Customer, during normal business hours, and upon twenty (20) days' prior written notice to ZEIT; *provided, however*, that in the event of a Security Incident, the twenty-day notice requirement will be waived and the parties will agree upon a reasonable, mutually agreeable time. Any inspection will be of reasonable duration and will not unreasonably interfere with ZEIT's day-to-day operations. All Independent Auditors are required to enter into a non-disclosure agreement containing confidentiality provisions reasonably acceptable to ZEIT and intended to protect ZEIT's and its customers' confidential and proprietary information. Customer will make (and ensure that any Independent Auditor makes) reasonable endeavors to avoid causing any damage, injury or disruption to ZEIT's premises, equipment, personnel and business in the course of such an audit or inspection. To the extent that Customer or any Independent Auditor causes any damage, injury or disruption to the ZEIT's premises, equipment, personnel and business in the course of such an audit or inspection, Customer will be solely responsible for any costs associated therewith.

12. Transfers of Personal Data.

12.1. Regions. Customer may specify the location(s) where Customer Data will be Processed within the ZEIT Network, including the EU (Brussels) Region, or the US (San Francisco) Region (each a "Region"). Once Customer has made its choice, ZEIT will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the

Standard Contractual Clauses.

12.2. Application of Standard Contractual Clauses. The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA or the United Kingdom, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data. The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA or the United Kingdom. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if ZEIT: (i) is located in the U.S. and has received Privacy Shield certification; *provided, however*, that if the EU deems Privacy Shield inadequate or ZEIT's certification lapses during the term of the Services Agreement and this DPA, the parties will promptly ensure compliance with the Standard Contractual Clauses, or (ii) has adopted, at its sole discretion, Binding Corporate Rules for Processors or an alternative recognized compliance standard for the lawful transfer of Personal Data outside the EEA or the United Kingdom. As of the data of ZEIT's signature to this DPA, ZEIT is certified under the Privacy Shield.

13. Termination of the DPA. This DPA will continue in force until the termination of the Services Agreement (the "Termination Date").

14. Return or Deletion of Customer Data. Up to the Termination Date, Customer will continue to have the ability to retrieve or delete Customer Data in accordance with Section 2.1 and this Section. For 90 days following the Termination Date, Customer may retrieve or delete any remaining Customer Data from the Services, subject to the terms and conditions set out in the Services Agreement, unless prohibited by law or the order of a governmental or regulatory body or it could subject ZEIT or its Affiliates to liability. No later than the end of this 90-day period, Customer will close all ZEIT accounts. ZEIT will delete Customer Data when requested by Customer by using the Service controls provided for this purpose by ZEIT.

15. Duties to Inform. Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by ZEIT, ZEIT will inform Customer without undue delay. ZEIT will, without undue delay, notify all relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

16. Liability. The total liability of ZEIT (and its respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the lesser of: (a) the limitation of liability for aggregate or direct damages set forth in the Services Agreement and (b) one hundred thousand dollars.

17. Choice of Law. Without prejudice to any requirements under the GDPR, or clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the EU Standard Contractual Clause Agreement, the parties hereby submit to the choice of venue and jurisdiction stipulated in the Services Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; *provided, however*, that the parties agree that this DPA shall be governed by the laws of Ireland.

18. Entire Agreement; Conflict. Except as amended by this DPA, the Services Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Services Agreement and this DPA, the terms of this DPA will control.

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER

Signature: .....

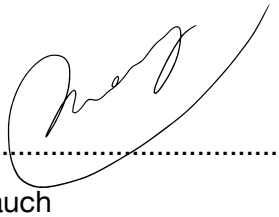
Print Name: .....

Title: .....

Customer Legal Name: .....

Date: .....

ZEIT Inc.



Signature: .....

Guillermo Rauch
Chief Executive Officer
February 28th, 2020

Annex 1
ZEIT Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Services Agreement.

1. Information Security Program. ZEIT will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the ZEIT Network, and (c) minimize security risks, including through risk assessment and regular testing. ZEIT will appoint one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1. Network Security. The ZEIT Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. ZEIT will maintain access controls and policies to manage what access is allowed to the ZEIT Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. ZEIT will maintain corrective action and incident response plans to respond to potential security threats.

2. Continued Evaluation. ZEIT will conduct periodic reviews of the security of its ZEIT Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. ZEIT will continually evaluate the security of its ZEIT Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by periodic reviews.