GDPR ADDENDUM (ON PREMISE)
"GDPR ADDENDUM"

This GDPR Addendum, forms an integral part of the Agreement between Annotate Software Limited and the Customer (as listed in the Order Form). As this is an On-Premise Installation, the GDPR Addendum (Hosted) and Privacy Policy available at https://www.annotate.co/legal-terms.html do not apply to the Agreement.

Since the Annotate Software is downloaded and installed in the Customer's environment and the Customer Data is hosted in the Customer's environment, it is not anticipated that Annotate will process Customer Personal Data under the Agreement. Annotate can only access Customer Personal Data if explicitly authorised by the Customer. From time-to-time Customer may request Annotate to provide Support Services and whilst in the majority of cases this can be performed without requiring Annotate to process Customer Personal Data, processing may occasionally be required. This GDPR Addendum applies to Customer Personal Data processed by Annotate under the Agreement.

1. Definitions

1.1. Any defined terms in this GDPR Addendum shall be interpreted in accordance with the On-Premise Customer Terms of Service ("Terms of Service").

1.2. The following additional defined terms shall apply in this GDPR Addendum:

Customer Personal Data	any Personal Data within the Customer Data or data relating to an Authorised User which is processed by Annotate as a Data Processor on behalf of the Customer in connection with the performance of the Agreement.
Adequate Jurisdiction	means the UK, EEA, or a country, territory, specified sector or international organisation which ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, as set out in: • with respect to Personal Data relating to Data Subjects in the EEA, a decision of the European Commission. • with respect to Personal Data relating to Data Subjects in the UK, the UK Data Protection Act 2018 or regulations made by the UK Secretary of State under the UK Data Protection Act 2018.
Authorised Subprocessor	means any entity appointed by or on behalf of Annotate to process Customer Personal Data on behalf of the Customer in accordance with the terms of this GDPR Addendum.
Applicable Data Protection Laws	all national and international data protection and privacy laws and regulations (including, as applicable, UK, EU, Singapore and US DP Laws:) and any national implementing laws, regulations and secondary legislation, each as may be updated, amended or replaced from time to time, as applicable to the Customer or Annotate.
Data Breach	means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorised disclosure of Customer Personal Data.
Data Controller	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 Subject	an individual whose personal data is included in the Customer Personal Data. References in this GDPR Addendum to a Data Subject includes a "Consumer" as defined under US DP Laws.
Data Processor	shall be as defined under UK GDPR. References in this GDPR Addendum to a Data Processor includes a "Processor" as defined in the VCPDA and CPA, "Service Provider" as defined in the CCPA, and "Data Intermediary" as such term is defined in the PDPA..
Annotate Personnel	means employees contractors of Annotate or its Affiliates.
Personal Data	means any data which directly or indirectly identifies a natural living individual.

Process	means any operation performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; "processed" shall be construed accordingly.
UK, EU, Singapore and US DP Laws	• EU DP Laws means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), • UK DP Laws means UK DPA (Data Protection Act) 2018 ("**DPA**") and the UK GDPR ("**UK GDPR**"). • Singapore DP Laws means the Personal Data Protection Act 2012 ("**PDPA**") • US DP Laws includes, as applicable, the California Consumer Privacy Act 2018 ("**CCPA**"), California Privacy Rights Act 2020, Virginia Consumer Data Protection Act ("**VCDPA**"), and Colorado Privacy Act ("**CPA**").
Standard Contractual Clauses or "SCCs"	means Module Three (processor to processor) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914)
UK ICO Addendum	means the UK ICO issued International Data Transfer Addendum to the Standard Contractual Clauses.

2. Applicability and Compliance with Applicable Data Protection Laws

2.1. Since the Annotate Software is downloaded and installed in the Customer's environment and the Customer Data is hosted in the Customer's environment, it is not anticipated that Annotate will process Customer Personal Data under the Agreement. Annotate can only access Customer Personal Data if explicitly authorised by the Customer. From time-to-time Customer may request Annotate to provide Support Services and whilst in the majority of cases this can be performed without requiring Annotate to process Customer Personal Data, processing may occasionally be required. This GDPR Addendum applies to Customer Personal Data processed by Annotate under the Agreement.

2.2. Each of Annotate and the Customer shall comply with their obligations under Applicable Data Protection Laws.

2.3. Customer Personal Data: The Customer and Annotate acknowledge in respect of Customer Personal Data processed by Annotate the Customer is a Data Controller and Annotate is a "Data Processor".

3. Scope and Particulars of Processing

3.1. Annotate shall process Customer Personal Data on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, and as otherwise necessary to perform its obligations under the Agreement, and (b) as necessary to comply with applicable law; and (c) as otherwise agreed in writing between the Customer and Annotate ("**Permitted Purpose**").

3.2. CCPA: For the avoidance of doubt, and notwithstanding any other term of the Agreement, the Customer discloses Customer Personal Data to Annotate solely for a valid business purpose and for use in accordance with the Permitted Purpose. Annotate is prohibited from: (i) selling Customer Personal Data; (ii) retaining, using, or disclosing Customer Personal Data for a commercial purpose other than providing the Services; (iii) retaining, using, or disclosing the Customer Personal Data outside of the Agreement between Annotate and Customer, (iv) combining the Customer Personal Data with personal data of Annotate's other customers. Annotate understands the prohibitions outlined in this Clause 3.1.

3.3. The Particulars of Processing set out below specifies the duration of the processing, the nature and purpose of the processing, types of Personal Data and categories of Data Subjects within the scope of the Customer Personal Data. The Parties Annotate does not inform or control the scope of Customer Personal Data and that this is determined by the Customer. Annotate does not actively or routinely monitor, assess, or verify the scope of the Customer Personal Data.

Duration of Processing	As per the Agreement.
Nature/purpose of Processing	As per the Agreement.
Types of Personal Data	This is controlled and determined by the Customer. Annotate does not independently have access to Customer Personal Data and Customer's authorisation is required. - Personal Data may include the following and other types of Personal Data: names, dates of birth, postal addresses, email addresses, telephone numbers, online identifiers, contractual details, education

	details, financial details special categories of Personal Data and other types of Personal Data contained in the Customer Data. - Sensitive Personal Data: any Sensitive Personal Data contained in the Customer Data.
Categories of Data Subjects	This is controlled and determined by the Customer and Authorised Users.

3.4. The Customer is responsible for ensuring it has all rights, consents and permissions necessary to submit the Customer Personal Data to Annotate for processing by Annotate in accordance with the terms of the Agreement.

3.5. Annotate shall process the Customer Personal Data as required for Annotate to provide the products and services and perform its obligations within the scope of an Agreement. In addition, Annotate may process Customer Personal Data as necessary to comply with Annotate's obligations under Applicable Data Protection Laws, however Annotate shall notify the Customer in advance of the additional grounds and requirements for the processing unless Annotate is legally prohibited from doing so.

3.6. Annotate shall process the Customer Personal Data solely in accordance with the Agreement. The Agreement constitutes the Customer's documented instruction to Annotate regarding the processing by Annotate of the Customer Personal Data.

3.7. Taking into account the nature of the processing to be performed by Annotate and the information available to Annotate, Annotate shall notify the Customer if in Annotate's reasonable opinion, the Customer's instructions regarding the processing of Customer Personal Data is likely to infringe Applicable Data Protection Laws. Annotate reserves the right, without liability and on reasonable notice, to refuse to comply with the Customer's instructions (including, at Annotate's discretion, suspension or termination of the products and services being supplied under an Agreement) where Annotate reasonably believes that compliance with such instructions will cause Customer or Annotate to breach Applicable Data Protection Laws.

3.8. Taking in to account the nature of the processing to be performed by Annotate and the information available to Annotate, Annotate shall provide information and assistance reasonably requested by the Customer as needed for the Customer to comply with its obligations under Articles 32 through to Article 36 of the GDPR and corresponding obligations under the UK GDPR.

3.9. Annotate shall, to the extent legally permitted, promptly notify the Customer if Annotate receives any request from a Data Subject to exercise that Data Subject's legal data protection and privacy rights afforded to the Data Subject under Applicable Data Protection Laws. Customer is solely responsible for fulfilling a Data Subject request. Since the Customer is hosting the Annotate Software in the Customer's environment, the Customer has ultimate control in respect of the Annotate installation including but not limited to setting, amending or removing functionality within a Workspace, Topic or Chat (as may be permitted under this Contract), enabling, reinstating, amending or revoking Authorised Users' account access and privileges, and other related matters as set out in the Terms of Service.

4. . Technical and Organisation Security Measures

4.1. The Customer will be hosting the Annotate Software in the Customer's environment and therefore the Customer controls the Customer Personal Data (if any) which the Customer elects to supply or otherwise make available to Annotate and Annotate does not require access to the Customer Data (including Customer Personal Data) in order for Customer and End Users to access the Annotate Software.

4.2. Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as risks to the rights and freedoms of natural persons, Annotate implements and maintains technical and organisational measures to ensure a level of security appropriate to those risks, including the following (as appropriate): the pseudonymisation and encryption of personal data; preserving the ongoing confidentiality, integrity, availability and resilience of processing systems and services; preserving the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and process for regularly testing, assessing and evaluating the effectiveness of those security measures.

4.3. In assessing the appropriate level of security to be taken in the Clause above, Annotate will take account of the risks from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Customer Personal Data transmitted, stored or otherwise processed by or on behalf of Annotate. Details of Annotate's current security protocols will be supplied on request and this information shall be considered Annotate's Confidential Information under the Agreement. Annotate may modify its security protocols from time to time.

4.4. Annotate does not independently have access to Customer Personal Data and Customer's authorisation is required. Annotate will ensure that Annotate personnel with access to Customer Personal Data are made aware of their data protection and security obligations and are bound by a duty of confidentiality in respect of the Customer Personal Data.

5. Sub-Processors

5.1. The Customer will be hosting the Annotate Software in the Customer's environment and therefore the Customer controls the Customer Personal Data (if any) which the Customer elects to supply or otherwise make available to Annotate and Annotate does not require access to the Customer Data (including Customer Personal Data) in order for Customer and End Users to access the Annotate Software. As at today, no Subprocessors are engaged by Annotate to process Customer Personal Data.

5.2. If Annotate intends to engage a Subprocessor (or replace a Subprocessor), Annotate will notify the Customer via email at least 30 days in advance of the new Subprocessor's engagement.

5.3. Customer may object to Annotate's appointment or replacement of a Subprocessor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to the Subprocessor not being compliant with Applicable Data Protection Laws. In such an event, the Customer and Annotate agree to discuss commercial reasonable alternative solutions in good faith. If Annotate and the Customer cannot reach a resolution within sixty (60) days, (a) Annotate shall not engage the objected to Subprocessor to process Customer Personal Data or transfer any Customer Personal Data to the objected to Subprocessor and (b) Annotate may suspend or terminate the applicable products and services being supplied under the Agreement in which the objected to Subprocessor would be involved without further liability to the Customer; such termination by Annotate shall be without prejudice to any Fees payable or incurred by Customer prior to suspension or termination. If no objection has been raised prior to Annotate replacing or appointing a new Subprocessor, the Customer will be deemed to have approved the engagement of the new Subprocessor who shall then be an "Authorised Subprocessor".

5.4. In respect of any Authorised Subprocessor engaged by Annotate:

5.4.1. Annotate will ensure that the arrangement between Annotate and each Authorised Subprocessor is governed by a written agreement under which the Subprocessor subject to the same or similar obligations as are set out in this Data Protection Addendum.

5.4.2. Annotate will ensure that the Authorised Subprocessor provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of Applicable Data Protection Laws.

5.5. At the Customer's request, Annotate shall provide a copy of the written agreements (including amendments) with an Authorised Subprocessor. To the extent necessary to protect business secret or confidential information or other commercially sensitive information of Annotate or the Authorised Subprocessor, Annotate may redact the text of the agreement between Annotate and the Authorised Subprocessor prior to disclosing it to the Customer. All information provided under this Clause shall be considered Annotate's Confidential Information under the Agreement.

5.6. Annotate will remain liable for any breach of Applicable Data Protection Laws and this Data Protection Addendum which is caused by an act, error or omission of its Subprocessors.

5.7. Annotate may in the future put in place a mechanism for the Customer to subscribe to notifications about addition or replacements to the Subprocessors engaged by Annotate. Once available, this will replace the notification process at Clause 5.2 above. Annotate shall provide the Customer with information on how to subscribe to such notifications. Provided Annotate has informed Customer on how to subscribe, the Customer shall be responsible for ensuring it subscribes to receive notifications regarding additions or replacements to the Subprocessor List. If the Customer has subscribed to receive notifications regarding the addition or replacement of Subprocessors on the Subprocessor list, Annotate will provide notifications to the Customer of any such changes at least 30 days prior to the change.

6. Data Breach and Notification

6.1. Annotate shall (i) notify the Customer without undue delay, but in no event later than twenty-four (24) hours after becoming aware of a Data Breach and (ii) take appropriate measures to address the Data Breach, including measures to mitigate any adverse effects resulting from the Data Breach. Annotate does not have access to the Customer Personal Data without the Customer's explicit authorisation.

6.2. To enable Customer to notify a Data Breach to supervisory authorities or Data Subjects (as applicable), Annotate will cooperate with and assist Customer by including in the notification under Section 6.1 such information about the Data Breach as Annotate is able to disclose to Customer, taking into account the

nature of the processing, the information available to Annotate, and any restrictions on disclosing the information, such as confidentiality.

6.3. The obligations of Annotate under Clause 6.2 shall not apply to a Data Breach which is caused by the Customer, End Users and/or non-Annotate products and services and/or relating to or concerning Customer environment factors such as but not limited to Customer selected or deployed hardware, servers, operating systems, networks and/or any other Customer IT infrastructure ("**Customer Environment Incidents**"). Annotate may, at Annotate's discretion, and if requested by the Customer, provide commercially reasonable assistance to the Customer in connection Customer Environment Incidents but the Customer shall be responsible for any costs arising from Annotate's provision of such assistance including payment of Annotate's fees for the assistance supplied.

7. Return and Deletion of Customer Personal Data

7.1. On termination of the Agreement all processing of the Customer Personal Data by Annotate shall cease unless continued Processing is required under law and in such a case Annotate shall inform Customer of the legal grounds mandating continued processing.

7.2. On termination of the Agreement, if Annotate has any Customer Personal Data in its possession (this is not anticipated since the Customer is hosting the Annotate Software in its own environment) Annotate shall delete the Customer Personal Data in accordance with the terms of the Agreement.

7.3. On Customer's request, Annotate shall provide written certification to Customer that it has complied with this Clause 7.

8. Audits

8.1. Annotate shall make available to Customer all information necessary to demonstrate Annotate's compliance with its obligations set out in this GDPR Addendum and allow for and contribute to audits (at the Customer's cost), including inspections in respect of the same, conducted by Customer or another auditor mandated by Customer, provided that any audits (including inspection) performed by or on behalf of the Customer or its Affiliates across all Agreements shall be limited to one (1) per annum and shall not, unless otherwise agreed by Annotate, exceed one (1) Business Day; Customer and/or its Affiliates (as applicable) shall, if requested by Annotate, procure that its third-party auditors enter into confidentiality undertakings with Annotate that are no less onerous than those set out in the Agreement. Any information disclosed by Annotate in connection with or during the audit shall constitute Annotate's Confidential Information; Customer and its Affiliates (as applicable) provide reasonable prior notice of such request for an audit or inspection; Customer and its Affiliates (as applicable) shall take steps to ensure that any such audit or inspection shall not be unreasonably disruptive to Annotate's business; and nothing in this Clause shall permit Customer or its Affiliates or their appointed auditors to make unaccompanied site visits to Annotate's premises, or to logically access Annotate's systems.

8.2. In deciding on a review or an audit, the Customer may take into account relevant certifications held by Annotate.

9. Location of Processing

9.1. Annotate does not host the Customer Personal Data as the Annotate Software is installed in the Customer's own environment.. Annotate does not have access to Customer Personal Data unless access is explicitly granted by the Customer. Annotate will only access the Customer Personal Data if authorised by the Customer and will only use it for the Permitted Purpose.

9.2. If Annotate notifies the Customer about the engagement of an Authorised Subprocessor, and so long as the Customer has not objected to the engagement in accordance with the terms of this GDPR Addendum. the Customer authorises Annotate to transfer Customer Personal Data to an Authorised Subprocessors for processing in accordance with the Permitted Purpose and provided that such transfer is always in accordance with the terms of this GDPR Addendum and Applicable Data Protection Laws. In the event the Authorised Subprocessor is located in a country outside of the UK or EEA and that country is not deemed to be an Adequate Jurisdiction, Annotate will enter into the Standard Contractual Clauses or UK ICO Addendum (as applicable) with the Authorised Subprocessor.