

CLOUD SERVICES TRIAL AGREEMENT

YOU SHOULD READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE USING ANY SAG ALFABET GMBH CLOUD SERVICES TO WHICH THESE TERMS AND CONDITIONS APPLY (“**CLOUD SERVICES**”). THE USE OF ANY CLOUD SERVICES WILL INDICATE ACCEPTANCE OF THESE TERMS AND CONDITIONS AND CONSENT TO BE BOUND BY THEM. YOU HAVE AUTHORITY TO ACT ON BEHALF OF YOUR COMPANY (“**CUSTOMER**”) IN DEALING WITH THE RELEVANT SAG ALFABET GMBH GROUP COMPANY (“**SUPPLIER**”).

1 USE OF SERVICES

- 1.1 **Access to Cloud Services:** Supplier grants the Customer a right to access and use the Cloud Services for evaluation, testing and proof of concept purposes only for 30 days (“**Trial Term**”) subject to the availability of third party infrastructure, required and emergency maintenance, availability of third party networks and communications facilities and force majeure events.
- 1.2 **Exit Terms:** Access to the Cloud Services will be removed upon expiry of the Trial Term. Within 30 days after termination (the “**Exit Period**”):
 - (a) Customer will be able to download a final backup of the Customer Data and IS Packages containing developed artifacts; and
 - (b) on request, Supplier will provide Additional Metadata (e.g. audit logs and execution results) in .csv format. After the Exit Period, Supplier will delete the Customer’s environment/tenant, dedicated virtual servers and the Customer Data following industry-standard practices.
- 1.3 **Restrictions:** The right to access and use the Cloud Services is subject to the following restrictions:
 - (a) Customer shall not:
 - commercially exploit or make the Cloud Services available to any third party
 - access or use the Cloud Services other than in compliance with all applicable laws and regulations;
 - interfere with or disrupt the integrity or performance of the Cloud Services or the data contained therein;
 - conduct penetration testing other than by agreement with Supplier;
 - (b) the Customer shall obtain any consents and authorizations necessary for the Customer’s use (and the Supplier’s provision) of the Cloud Services.
- 1.4 **Termination:** Either Party may terminate this Agreement with immediate effect by written notice.

2 CUSTOMER INFORMATION

- 2.1 **Customer Access:** The Customer is responsible for the access to the Cloud Services and is responsible for maintaining the confidentiality of its access methods such as usernames and passwords and agrees to notify the Supplier via the Cloud Services support channel if a password is compromised. The Customer is responsible for all activities that occur under its Account.
- 2.2 **Metadata, Customer Data and Customer Personal Data:** The Cloud Services will gather and transmit certain technical information, Account information, and metadata associated with the Customer’s access and use of the Cloud Services, including application telemetry, IP addresses, IP configurations, stored sessions, open ports, Account credentials, network metadata, and device operating system, status, version and configuration (collectively “**Metadata**”). Metadata will not include any of the actual Customer Data processed with the Cloud Services. With the exception of Metadata the Customer shall own all content, information, materials, and intellectual property provided in its unaltered form by Customer in connection with Customer’s use of and access to the Cloud Services (“**Customer Data**”). The obligations of the parties in connection with the processing of any Customer Data that qualify as personal data according to Art. 4 No. 1 of the General Data Protection Regulation (GDPR) (“**Customer Personal Data**”) including the applicable technical and organizational measures that Supplier is required to implement and maintain to protect Customer Personal Data, shall be as set out in the Data Processing Agreement entered into between the Parties.
- 2.3 **Customer Responsibility for Customer Data:** The Customer is solely responsible for all Customer Data provided, or uploaded to, stored in or transmitted through the Cloud Services and the use of the Cloud Services by the Customer and its Users.
- 2.4 **Supplier Access to Customer Data and Metadata:** The Supplier will not use or access the Customer Data associated with the use of and access to the Cloud Services by the Customer in the ordinary course of the provision of the Cloud Services and has policies and data protection controls in place which prohibit cloud operations staff from accessing Customer Data unless explicitly authorised and instructed by the Customer administrator. Should the Supplier require such access it may do so only with the prior instruction of the Customer (not to be unreasonably withheld or delayed in any of the circumstances referred to below). Customer hereby instructs and accordingly grants to the Supplier a worldwide, irrevocable, non-transferable, non-assignable (except as permitted under this Agreement), sub-licenseable, non-exclusive license to access, retrieve, store, copy, display, distribute, transmit and otherwise use the Customer Data associated with the Cloud Services:
 - (a) in connection with maintaining, providing and/or making available the Cloud Services;
 - (b) as reasonably required in order to cooperate with legitimate governmental requests, subpoenas or court orders provided that Supplier gives Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Supplier is legally prohibited from doing so;
 - (c) as otherwise required in order to protect the Supplier’s systems and the Customer; and
 - (d) otherwise for the purposes of ensuring the integrity and operation of the Supplier’s business and systems.The Customer hereby consents to the use by the Supplier of the Metadata as reasonably required in connection with maintaining, providing and/or making available the Cloud Services.

3 AI COMPONENTS AND GENERATED CONTENT

- 3.1 **AI Generated Content:** The Cloud Services may include components that utilize artificial intelligence (“**AI**”) to generate content (“**AI Generated Content**”) either from user inputs or contextual information derived from content provided by the Customer. Supplier will automatically collect information associated with user inputs, augmented inputs, responses and results as part of Operational Data as defined under the clause “Operational Data, Feedback”. The AI Generated Content is provided “as is” and without any warranty of any kind, express or implied, including but not limited to any implied warranties of merchantability, fitness for a particular purpose and non-infringement. The Supplier makes no representations or warranties regarding the accuracy, completeness, reliability, or suitability of the AI Generated Content and shall not be liable for any damages and shall, to the fullest extent permitted by law, not be liable for any damages arising out of or in connection with the use of the AI Generated Content.
- 3.2 **Role as Integrator:** For the purposes of the AI Act, the Supplier acts solely as an integrator of AI components and does not develop or modify the underlying AI technologies. The Supplier’s role is limited to integrating these components into the Cloud Services.

3.3 Data Processing: AI Generated Content will require that Customer Data be transmitted to and temporarily stored and processed in locations other than the associated Data Storage Location referenced in this Agreement. The Supplier shall take reasonable measures to ensure the security and confidentiality of the Customer Data during such processing and Customer Data shall not be used to train, develop or improve any AI models without the Customer's explicit consent. The Customer further represents and warrants that the user inputs when using AI components do not contain any personal data as defined under Art. 4 GDPR. Customer shall indemnify the Supplier in full against any claims by third parties (including data protection supervisory authorities) arising from Customer's failure to comply with this clause.

3.4 Explicit Consent: By using the AI-Generated Content, the Customer acknowledges and agrees to the terms of this clause as well as the relevant terms of the respective AI provider (<https://aws.amazon.com/service-terms/> for AWS/Bedrock and <https://www.microsoft.com/licensing/terms/productoffering/onlineservices> for Azure AI).

4 DATAPROTECTION & SECURITY

4.1 Data Protection: The obligations of the parties in connection with the processing of any customer data that qualify as personal data according to Art. 4 No. 1 of the General Data Protection Regulation (GDPR) including the applicable technical and organizational measures that Supplier is required to implement and maintain to protect such personal data, shall be as set out in the Data Processing Agreement entered into between the Parties.

4.2 Cloud Privacy Policy: In order to provide the Cloud Services, the Supplier will access and use the Metadata in accordance with its then current Cloud Privacy Policy <https://www.alfabet.com/privacy>

4.3 Security: In performing the Cloud Services, Supplier:

- (a) will employ commercially reasonable security measures;
- (b) agrees to make reasonable commercial efforts to safeguard the personal data associated with the Customer Data from unauthorized access or use; and
- (c) will comply with its then current Cloud Information Security Policy as amended from time to time and available on request (subject to a written confidentiality agreement between the Parties). The Cloud Information Security Policy is designed along the requirements of ISO 27001.

5 CONFIDENTIALITY

5.1 Confidentiality: Each Party agrees:

- (a) to use Confidential Information only for the purposes described herein; and
- (b) not to reproduce Confidential Information and to hold it in confidence and protect it from dissemination to, and use by, any third party; and
- (c) not to create any derivative work from Confidential Information; and
- (d) to restrict access to the Confidential Information to its personnel, agents, sub-contractors and/or consultants, who need to have access to such Confidential Information and who have been advised of and have agreed in writing to treat such Confidential Information in accordance with this Agreement; and
- (e) to return or, at the disclosing party's discretion, destroy all Confidential Information of the other Party in its possession upon termination or expiration of this Agreement.

5.2 Exclusions: The restrictions shall not apply to Confidential Information that:

- (a) is publicly available or in the public domain at the time disclosed;
- (b) is or becomes publicly available or enters the public domain through no fault of the recipient;
- (c) is rightfully communicated to the recipient by persons not bound by confidentiality obligations with respect thereto;
- (d) is already in the recipient's possession free of any confidentiality obligations with respect thereto at the time of disclosure;
- (e) is independently developed by the recipient; or
- (f) is approved for release or disclosure by the disclosing Party without restriction.

5.3 Compliance with law permitted: Each Party may disclose Confidential Information to the limited extent required to comply with the order of a court or other governmental body or applicable law, including to make such court filings as it may be required to do, provided that it gives reasonable notice of the demand to allow the other Party to seek a protective order or other appropriate remedy (unless is legally prohibited from doing so).

6 INDEMNITY

6.1 Customer Indemnity: Customer shall indemnify, defend, and hold the Supplier harmless from any action brought by a third-party against the Supplier to the extent that it is proximately caused by an allegation that:

- (a) any access to or use of Customer Data with the Cloud Services; or
 - (b) modification or use of the Cloud Services with the Customer's applications;
- have infringed any intellectual property right or trade secret and pay those damages or costs related to the settlement of such action or finally awarded against the Supplier in such action, including but not limited to reasonable attorneys' fees, provided that the Supplier:
- promptly notifies Customer of any such action; and
 - gives Customer full authority, information, and assistance to defend such claim; and
 - gives Customer sole control of the defense of such claim and all negotiations for the compromise or settlement of such claim. Customer shall have the right to settle or compromise any such claim provided that such settlement or compromise does not impose any costs or material disadvantage to Supplier without Supplier's prior written consent.

7 LIMITATION OF LIABILITY

7.1 Warranty Disclaimer: The Customer acknowledges that the Cloud Services are provided "as is" without any warranty whatsoever solely for the Customer's evaluation. THE SUPPLIER DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.

7.2 Limitation of Liability: To the extent permitted by law, Supplier shall not be liable for any damages caused by the use of the Cloud Services.

8 GENERAL

8.1 Governing Law: This Agreement and all matters relating to the interpretation and effect of this Agreement are made and will be governed exclusively by and construed in accordance with the laws of Germany without giving effect to its conflicts-of-laws provisions and exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG). The parties consent and submit to exclusive personal jurisdiction, procedure and venue for legal disputes arising from or connected with this Agreement shall lie with the courts of Berlin-Charlottenburg, Germany. Arbitration processes are excluded.