FREE EDITION CLOUD SERVICES AGREEMENT

YOU SHOULD READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE USING ANY SOFTWARE AG 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 ATTEST THAT YOU HAVE AUTHORITY TO ACT ON BEHALF OF YOUR COMPANY ("**CUSTOMER**") IN DEALING WITH THE RELEVANT SOFTWARE AG GROUP COMPANY ("**SUPPLIER**").

1 USE OF SERVICES

1.1 **Access to Cloud Services**: Supplier grants Customer a non-exclusive, non-transferable, non-sublicensable right to access and use, except from a Prohibited Country, the Supplier web-based products and services identified in an Order Form ("**Cloud Services**"), including the then-current version of any user manuals and operating instructions generally provided with the Cloud Services (collectively, "**Documentation**"), for the term set out in the Order Form ("**Cloud Services Term**"). Customer may use the Cloud Services subject to the terms of this Agreement and solely for its internal use. Customer will not receive a copy of any programs listed in the Order Form. "**Prohibited Country**" means a country or territory that is the subject of sanctions administered or enforced by: i) DE/EU Embargo Country regulations on BAFA website, ii) US-EAR §740-Supplement No.1 - Group E:1/E:2 countries, iii) EAR-Rules , iv) OFAC restrictions v) German / EU - Embargo Countries on BAFA Website, vi) German National License Exception AG16 for software, vii) German Foreign Trade and Payment Ordinance §9 AWV, viii) Additional "National Security" related US-EAR §740-Supplement No.1 - Group D:1 countries or ix) additional "Arms Embargo" related US-EAR §740-Supplement No.1 - Group D:5 countries. "**Users**" of the Cloud Services mean employees or contractors of Customer who are authorized by Customer in accordance with the Agreement to access the Cloud Services using Customer's account credentials ("**Credentials**"). Customer is solely responsible for all User use of, and access to, the Cloud Services and the security of any Credentials and will immediately report to Supplier any suspected unauthorized use of the Cloud Services or Credentials. The terms and conditions of the Cloud Services may be amended from time to time with a 30-day advance notice to Customer.

1.2 **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;
- use the Cloud Services for military, para-military, police, border protection, intelligence service, arms, military purposes, nuclear power plants, nuclear technology (including production, operations, transport, delivery of such items), Internet and/or communication surveillance (incl. person tracking, face recognition functions) purposes.
- use the Cloud Services from a Prohibited Country

(b) the Customer shall obtain any consents and authorizations necessary for the Customer's use (and the Supplier's provision) of the Cloud Services.

1.3 **Termination**: Either Party may terminate this Agreement with immediate effect by written notice. Access to the Cloud Services will be removed upon termination of this Agreement. Thirty (30) days or more after such termination, Supplier shall delete Customer's environment/tenant, dedicated virtual servers and the Customer Data following industry standard practices.

2 CUSTOMER INFORMATION

2.1 **Customer Access**: The Customer is responsible for all User 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 **Suspension of Cloud Services:** Supplier may suspend Customer's access to the Cloud Services at any time, with or without cause. If Customer does not access the Cloud Services or has no activity in connection with the Cloud Services for a period of forty-five (45) consecutive days, Supplier may suspend Customer's access to the Cloud Services with a 30-day advance notification of such suspension.

2.3 **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, but not

necessarily limited to, 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 in connection to 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"). Supplier may introduce new features, such as user guidance and onboarding technology, that may be turned on by default. Customer agrees to use these features and allows their usage patterns to improve the overall product functionality. 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 organisational 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.

2.4 **Customer Responsibility for Customer Data**: The Customer is solely responsible for:

(a) all Customer Data provided, or uploaded to, stored in, or transmitted through the Cloud Services

(b) access to, and use of, Cloud Services by the Customer and its Users.

2.5 **Supplier Access to Customer Data and Metadata**: Absent Customer's consent or explicit direction, The Supplier shall 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. The Supplier 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). Notwithstanding the foregoing, 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 in connection with maintaining, providing and/or making available the Cloud Services.

3 SUPPLIER OBLIGATIONS

3.1 **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 http://www.softwareag.com/corporate/privacy.asp.

3.2 **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 unauthorised 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.

4 CONFIDENTIALITY

4.1 **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.

4.2 **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.

4.3 **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).

5 INDEMNITY

5.1 **Customer Indemnity**: Customer shall indemnify, defend, and hold the Supplier harmless from i) any liability arising from any breach of this clause by the Customer and ii) 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.

6 LIMITATION OF LIABILITY

6.1 **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 MERCHANTABLE QUALITY, AND FITNESS FOR A PARTICULARPURPOSE.

6.2 **Limitation of Liability:** TO THE EXTENT PERMITTED BY LAW NEITHER SUPPLIER, ITS SUBSIDIARIES OR AFFILIATES NOR ANY OF ITS LICENSORS SHALL BE LIABLE FOR ANY LOSS OR DAMAGE HEREUNDER, INCLUDING WITHOUT LIMITATION ANY INACCURACY OF DATA, LOSS OF PROFITS OR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7 GENERAL

7.1 **Governing Law:** This Agreement is governed by the laws of the State of New York, without giving effect to its conflicts-of-laws provisions and excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG) and the Uniform Commercial Code (UCC). The Parties consent to exclusive personal jurisdiction in the federal and state courts located in the Southern District of New York. In the event a dispute arising under this Agreement results in litigation, the non-prevailing Party will pay the court costs and reasonable attorneys' fees and expenses of the prevailing Party. Each Party waives all right to a jury trial in any proceeding arising out of this Agreement.

7.2 **Export Control.** Customer may not download, provide access to, and otherwise export or re-export the Cloud Services, in whole or in part to any third party in a Prohibited Country, except as explicitly allowed in this Agreement and in compliance with all applicable laws, regulations and restrictions (whether international, federal, state, local, or provincial). Software AG reserves the right to not perform any obligation under the Agreement if prohibited by such export control laws, regulations or restrictions.

8 DATA PROCESSING AGREEMENT

8.1 **Data Processing Agreement:** The obligations of the parties in connection with the processing of any data that qualifies as personal data according to art. 4 no. 1 of the General Data Protection Regulation (“Personal Data”) including the applicable technical and organizational measures that supplier is required to implement and maintain to protect Personal Data, will be as set out in the data processing agreement entered into between the parties (“Data Processing Agreement”).