CLOUD PRIVACY POLICY

This policy covers the privacy practices of Software AG and its subsidiaries ("**the Supplier**") with effect from 7th September 2016 in relation to the use of the Supplier's applications and services made available in the cloud ("**Cloud Services**") by customers or potential customers ("**the Customer**"). The Cloud Services include support, application, hosting, infrastructure management, platform development and storage of information in managed data centres as part of the service specific cloud based offering further described in the respective Cloud Services Attachment or other contract document. The Supplier's general privacy policy terms can be found here.

1 COLLECTED INFORMATION

1.1 **Introduction** : The Supplier may collect the types of information described below (collectively "**Information**") in connection with the creation and administration of the Customer's account to permit the Customer's use of the Cloud Services.

1.2 **Personal Information** : Personal information such as first name, last name, e-mail address, telephone, work address, IP address and other types of information pertaining to the digital footprint is information that the Supplier may collect from the Customer's use of the Cloud Services.

1.3 **Services Information** : Services information is information located on the systems of Supplier, user or third party (f.e. AWS) which allows the Supplier to perform the Cloud Services. "**Services Information**" includes information the Customer provides to the Supplier to administer the Cloud Services including the Customer's personal information, payment and billing information and/or support information which may include the Customer's operating system, registry information, customer code, and diagnostic information.

1.4 **Metadata** : 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 without limitation application telemetry, IP addresses, IP configurations, stored sessions, open ports, network metadata, and device operating system, status, version and configuration (collectively "**Metadata**"). For clarification, Metadata is used to operate the Cloud Services and will not include any Customer Data.

1.5 **Customer Data** : Customers may electronically submit 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**") for hosting and processing purposes.

2 INFORMATION ACCESS, STORAGE & RETENTION

2.1 **Access** : In accordance with the terms and conditions of the Customer's Cloud Services Agreement, the Supplier may access Information only for the purpose of providing the Cloud Services, preventing or addressing service or technical problems, in connection with a customer support matter, or as may be required by law. The Supplier's access to Information is based on job role or responsibility. The Customer controls access to Services Information and Customer Data by the Customer's users and end users and is responsible for any requests related to the personal information contained in its Customer Data. The Supplier will not review, share, distribute, or reference any Information except as provided in the terms and conditions between

the Customer and the Supplier, or as may be required by law.

2.2 **Transfers via Third Parties** : The Supplier contracts with Third Parties, such as Amazon Web Services, to host the Cloud Services. The hosting entity is identified in the Cloud Services Attachment or other contract document between the Supplier and the Customer.

2.3 **Access to Data from Inside and Outside the EU** : The Customer defines who accesses the Customer Data on Customer's behalf. Based on the delivery of 24 x 7 support, it may be necessary for Supplier to access the Services Information and Customer Data from EU countries including Germany and non-EU countries including Malaysia and the USA in connection with the provision of such support. Subject to the Terms & Conditions of the respective Cloud Service, Customer hereby explicitly agrees to such access limited to the foregoing purpose.

2.4 **Storage** : The Customer determines where its Services Information and Customer Data will be stored and chooses from a list of geographical region(s) listed on the Customer's Cloud Services Attachment. Back-ups of Customer Data will be stored in the same AWS region as the Data Storage Location defined in the respective Cloud Service Attachment, but for security reasons will be based in a different AWS availability zone.

2.5 **Retention** : The Services Information and Customer Data will be retained for the duration of the Cloud Services Term and any Cloud Service Renewal Term as defined in Cloud Services Attachments. The Supplier will delete the Services Information and any Customer Data no later than 40 days after the expiry or termination of the Cloud Services Agreement.

3 HOW INFORMATION IS COLLECTED AND WHAT IT IS USED FOR

3.1 **How Information is collected and what it is used for** : The Supplier uses the Information to perform the Cloud Services and below are some of the circumstances under which the Supplier may access, collect, analyze as well as use such Information.

3.2 **Service Offering** : In order to provide the Cloud Services, it may be necessary for the Supplier to access, store and retain Information for purposes such as service enablement, billing, client support, customization, training or other services.

3.3 **Performance Purposes** : In order to ensure satisfactory performance standards, security levels and enforcement of service level commitments it may be necessary for the Supplier to access the Customer's production, development or test environments or copies thereof. Supplier may only do so with the prior consent of the Customer on the basis set out in the respective Cloud Services Agreement.

3.4 **Maintenance, Fixes and Upgrade Purposes** : In order to upgrade the system to the latest version or to monitor system performance or to introduce issue fixes it may be necessary, without notice to the Customer, for the Supplier to access the Cloud Services and provide patches, updates and fixes.

3.5 **Communication Purposes** : In order to better serve the Customer, such as to validate user identity, to provide emergency notifications or to offer proactive support, or to communicate beneficial offers it may be necessary to engage with the Information directly. This may include access to Services Information for the purpose of reproducing an error or troubleshooting an incident.

3.6 **Compelled Disclosure** : The Supplier may be required to disclose information in response to a lawful request by public authorities, including to meet national security or law enforcement

requirements.

4 SECURITY

4.1 **Security** : The Supplier is committed to the security of the Customer Data and Information and has various policies and tools in place to ensure the physical, administrative and technical security of Customer Data and Information. The Supplier employs security practices and operating procedures that are compliant with standard industry practices or other practices as defined in the relevant Cloud Service Attachment (as applicable). The Supplier's security processes are reviewed on a regular basis by the Software AG Global Security and Privacy Committee, led by the Corporate Security Officer.

5 INFORMATION TRACKING

5.1 **Cookies and other tracking devices** : The Supplier may use common information gathering tools such as cookies which are small text files placed on a hard disk by a web server or web beacons (a transparent graphic image placed on Supplier's website used to monitor website user behaviour). These information gathering tools are used for storing user preferences, settings, authentication and to collect information for operational efficiency. Unless a person chooses to identify themselves through opening an account or responding to a promotional offer, a person remains anonymous to the Supplier even in the event of any tracking functionality used by Supplier. Cookies do not collect any personal data stored on any Customer hard drive or computer nor are cookies used to collect any personally identifiable information about a web user.

5.2 **Types of Cookies** : The Supplier uses two types of cookies: persistent and session cookies. Persistent cookies are used to allow the website to recognize users when they return to the website and to remember certain information about the user's preferences. Persistent cookies stay on a user's computer until they are deleted. Session cookies are used in order to allow a Customer to carry information across pages of the website, without having to re-enter such information. These cookies delete themselves automatically when the Customer leaves the web site or shuts down its web browser. Without these cookies, the Cloud Services cannot be provided.

5.3 **Consent**: To comply with current legislation, to the extent that tracking cookies are used in the provision of the Cloud Services, a user will be asked for consent to set the persistent cookies described above. In such case, either a pop-up message or other click-accept field will be made available to collect the user's consent. Once consent has been provided, the message will not appear again. A user is free to withdraw its consent at any time by altering its browser settings. To learn more about cookies see: www.allaboutcookies.org or http://www.youronlinechoices.com.

6 NOTIFICATION OF POLICY CHANGES

6.1 **Notification of Privacy Policy Changes** : The Supplier reserves the right to change this privacy statement. The Supplier will post notice of the material changes to this privacy policy through the Supplier's web sites at least thirty (30) business days prior to the change taking effect.

7 CORRECTING AND UPDATING CUSTOMER INFORMATION

7.1 **Correcting and Updating Customer Information** : Customer may update or change its

registration information by editing its user or organization record. To update a user profile, log into your Customer account with your user name and password. To update an organization's information, please login to the administrator account using the administrator's user name and password.

7.2 **Deleting Information** : To update Billing Information or have your registration information deleted, Customers should create a request in Empower, Supplier's customer support portal. Requests to access, change, or delete billing information or delete Customer Data will be handled within thirty (30) days.

8 COMPLIANCE

8.1 **Compliance with EU-US Privacy Shield Framework** : Supplier is a global corporation and has developed global information practices designed to assure Information is appropriately protected. Supplier and its U.S. subsidiaries comply with EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information from European Union member countries. Supplier has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/.

8.2 **Compliance with US-Swiss Safe Harbor Framework** : The Supplier complies with the US-Swiss Safe Harbor Framework as set set forth by the US Department of Commerce regarding the collection, use and retention of personal information from Switzerland. Supplier has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement. If there is any conflict between the policies in this privacy policy and the Safe Harbor Privacy Principles, the Safe Harbor Privacy Principles shall govern. To learn more about the US-Swiss Harbor Framework, and to view our certification page, please visit http://www.export.gov/safeharbor/.

9 RECOURSE

9.1 **EU/EEA Individuals** : In compliance with the EU-US Privacy Shield Principles, the Supplier commits to resolve complaints about your privacy and our collection or use of your personal information. European Union individuals with inquiries or complaints regarding this privacy policy should first contact the Supplier at:

Data Protection Officer
Uhlandstrasse 12
64297 Darmstadt, Germany
E-mail: privacy@softwareag.com

The Supplier has further committed to refer unresolved privacy complaints under the EU-US Privacy Shield Principles to JAMS, an independent alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://www.jamsadr.com/file-an-eu-us-privacy-shield-or-safe-harbor-claim for more information and to file a complaint.

If your complaint is not resolved by contacting the Supplier or through the independent dispute resolution process, you may choose to invoke binding arbitration before the Privacy Shield Panel

to be created by the U.S. Department of Commerce and the European Commission or may contact your local Data Protection Authority. Supplier is subject to the investigatory and enforcement powers of the United States Federal Trade Commission.

9.2 **Swiss Individuals** : In compliance with the US-Swiss Safe Harbor Principles, the Supplier commits to resolve complaints about your privacy and our collection or use of your personal information. Swiss individuals with inquiries or complaints regarding this privacy policy should first contact the Supplier at:

Data Protection Officer
Uhlandstrasse 12
64297 Darmstadt, Germany
E-mail: privacy@softwareag.com

The Supplier has further committed to refer unresolved privacy complaints under the US-Swiss Safe Harbor Principles to JAMS, an independent alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://www.jamsadr.com/file-an-eu-us-privacy-shield-or-safe-harbor-claim for more information and to file a complaint.