PRIVACY POLICY FOR CLOUD & MANAGED SERVICES

This policy covers the privacy practices of Software AG and its subsidiaries ("**the Supplier**") with effect from 28th June 2017 in relation to the use of the Supplier's applications and managed services made available via the internet ("**Services**") by customers or potential customers ("**the Customer**"). These Services include support, application, hosting, infrastructure management, platform development and storage of information in managed data centers 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 statement can be found at https://www.softwareag.com/corporate/privacy.asp.

1 INFORMATION COLLECTED

The Supplier and its service providers may collect both personal information (defined below) and nonpersonal information ("Information") in connection with Customer's access and use of the Services. Personal information is information that either identifies an individual or relates to a specific individual, and includes without limitation, a person's name, physical address, telephone number, email, company affiliation, and in some jurisdictions an IP address. Nonpersonal information is information that does not reveal a person's specific identity or relates to a specific individual and may include electronic interaction information, geographic or geo-location information, statistical and aggregated information. While statistical and aggregated information may be derived from personal information the Supplier will anonymize any personal information prior to sharing this information with third parties.

2 INFORMATION ACCESS, SHARING, STORAGE & RETENTION

2.1 **Access**: In accordance with the terms and conditions of the Customer's Services Agreement, the Supplier may access Information for the purpose of providing the Services, preventing or addressing service or technical problems, in connection with a Customer support matter, to improve the Services provided to Customer, 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 Customer data uploaded, processed, and transmitted through the Services by the Customer's users and end users and is responsible for any requests related to the personal information contained in its Customer data.

2.2 **Information Shared with Service Providers**: The Supplier contracts with third parties to administer, host, distribute, resell, and/or support the Services. The hosting entity is identified in the cloud services attachment or other contract document between the Supplier and the Customer. These third-party services providers have access to personal information only for the limited and specific purpose of performing services on the Supplier's behalf and are expressly obligated not to disclose or use personal information for any other purpose. When the Supplier uses service providers to process personal information received in reliance on the Privacy Shield Principles, the Supplier is responsible if that service provider processes Information in violation of the Privacy Shield Principles (unless the Supplier can prove that it is not responsible for the service provider's action that violated the Privacy Shield Principles).

2.3 **Information Disclosed in Connection with Business Transactions**: With the exception of Customer data, Information that the Supplier collects, including personal information, is considered to be a business asset. Therefore, in due course of any bankruptcy or as a result of a transaction such as a merger, acquisition, sale, joint venture, assignment, transfer or other disposition of all or any portion of the Supplier's business, assets, or stock, Information may be disclosed or transferred to the third-party in connection with the transaction.

2.4 **Information Disclosed for the Supplier's Protection and the Protection of Others**: The Supplier maintains policies to protect its Customers from privacy violations by individuals, entities or government actors, and to contest claims that the Supplier believes to be invalid under applicable law. However, it is also the Supplier's policy to cooperate with government and law enforcement official requests. Accordingly, the Supplier reserves the right to disclose any Information as the Supplier, in its sole discretion, believes necessary: (i) to satisfy or comply with any applicable law, regulation or legal process or to respond to lawful requests, including subpoenas, warrants or court orders; (ii) to protect the Supplier's property, rights and safety and the rights, property and safety of third parties or the public in general; and (iii) to prevent or stop activity the Supplier considers to be illegal or unethical.

2.5 **Information Disclosed With Customer Consent**: At the Customer's express request and consent the Supplier will share Information with third-party sites or platforms.

2.6 **Supplier Access to Customer Data**: Based on the delivery of 24 x 7 support or in the performance of professional services, it may be necessary for the Supplier to access personal information and Customer data from EU countries (Germany, Bulgaria) and non-EU countries (Malaysia, Australia, USA) in connection with the provision of such services and support. Customer hereby explicitly agrees to such access limited to the foregoing purposes. If Supplier's access to personal information and Customer data results in the transfer of personal information from the EU and/or Switzerland to the U.S., respectively, the Supplier relies on the following legal mechanisms for such transfer: the EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Principles.

2.7 **Storage**: The Customer determines where its Customer data will be stored based on a list of available geographical region(s) listed on the Customer's cloud services attachment or other contract document. Back-ups of Customer data will be stored in the same region as the data storage location identified on the respective cloud service attachment or other contract document.

2.8 **Retention**: The Supplier will retain any Customer Information collected for as long as it is needed to provide the Services, as needed for the purposes outlined in this Privacy Policy or, at the time of collection, as necessary to comply with the Supplier's obligations (e.g., to honor opt-outs), resolve disputes, and enforce agreements, or to the extent required and permitted by law. The Supplier will delete Customer data no later than 30 days after the expiry or termination of the Customer's cloud services agreement unless otherwise agreed between the parties or local regulations require a longer retention period. At the end of the applicable retention period, the Supplier will delete Customer Information and Customer data in a manner designed to ensure that it cannot be reconstructed or read.

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 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 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 Services environment.

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 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 Information for the purpose of reproducing an error or troubleshooting an incident.

4 SECURITY

The Supplier is committed to the security of Customer Information and has various policies and tools in place to ensure the physical, administrative and technical security of such Customer 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 or contract document (as applicable). The Supplier's security processes are reviewed on a regular basis by Software AG's Security Council, 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.

5.2 **Types of Cookies** : The Supplier uses session cookies. 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 Services cannot be provided. To learn more about cookies see: www.allaboutcookies.org and www.youronlinechoices.com.

6 NOTIFICATION OF POLICY CHANGES

The Supplier reserves the right to change this privacy statement. The Supplier will post notice of updates or material changes to this privacy policy through the Supplier's web sites for a period of thirty (30) days. The updated policy is also added to the Supplier's customer portal, Empower, where Customers who subscribe to Services will be notified of any changes. If Supplier's changes to its privacy policy materially impact the use or collection of personal information Supplier will notify Customer, and Customer will have a choice as to whether Supplier may continue to collect or use the its personal information in such a manner.

7 CORRECTING AND UPDATING CUSTOMER INFORMATION

7.1 **Accessing, Correcting, and Updating Information** : The Customer may access, update or change its registration information by editing its user or organization record. To update a user profile, log into the Customer account with the user's 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, the Customer should create a request in Empower, the 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 WITH PRIVACY SHIELD FRAMEWORKS

Supplier complies with the EU - U.S. Privacy Shield Framework and the Swiss – U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States, respectively. The Supplier has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield Frame work and its Principles, and to view our certification, please visit https://www.privacyshield.gov/.

9 RECOURSE

EU or Swiss Individuals. In compliance with the EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Frameworks, the Supplier commits to resolve complaints about Customer privacyand our collection or use of personal information. European Union and Swiss individuals with inquiries or complaints regarding this privacy policy should first contact the Supplier at:

Data Protection Officer
Uhlandstraße 12
64297 Darmstadt, Germany
Email: privacy (at) softwareag.com

The Supplier has further committed to refer unresolved privacy complaints under the EU - U.S. Privacy Shield and the Swiss – U.S. 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/eu-us-privacy-shield for more information and to file a complaint.

If the 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.