Security Compliance Addendum

The existing agreement of between Software GmbH (or one of its affiliated companies) for the provision of Software and/or associated services between Supplier and Customer (the "**Agreement**") is supplemented by this Security Compliance Addendum (the "**SCA**") referred to herein, which is incorporated into the Agreement by reference.

This SCA describes the security standards and controls that Supplier has implemented to protect Supplier's digital assets and the Customer's data that is stored and processed in connection with the Software and/or associated services provided pursuant to the Agreement.

Supplier may change or add to the terms and conditions to the SCA from time to time for legal, security or other substantive reasons, provided always that any amendments to the terms of the Security Compliance Addendum will not impact in any materially adverse manner on the provisions and requirements set out in this SCA .

The most recent version of the SCA will be made available to Customers at: https://www.softwareag.com/en_corporate/tc/SAGDeutschlandGmbH-Security-Compliance-Regulatory-Addendum

1 Defined Terms.

Capitalized terms used in this Security Compliance Addendum but not otherwise defined herein will have the meanings given to them in the Agreement and include the following:

1.1 "Regulator"

This means a governmental agency with supervisory rights and jurisdiction, as provided under applicable law or regulations, over Customer or Supplier, as it applies to Customer's use of the Software and/or associated services.

1.2 "Security Documentation"

This means Supplier's then current documentation regarding its security, operational, and related controls is made generally available to Supplier's Customers from time to time. Security Documentation is Supplier Confidential Information. Supplier will not reduce the overall security standards set forth in the Security Documentation to a materially adverse extent.

These security standards include, but are not limited to, the Self-Service documentation made available to Customer at Supplier's trust portal at:https://www.softwareag.com/en_corporate/company/trust-portal.html

1.3 "Critical or Important Services"

Customer defines critical or important services as part of it's regulatory obligations, applying the proportionality principle if applicable, and in the context of the Supplier relationship and the outcome of its risk assessment.

2 Description of Services

Customer and Supplier shall cooperate to ensure that the description of services is kept up to date and for the purposes of determining whether the cloud services are within the definition of critical or important services regarding compliance to the applicable regulation.

2.1 Usage Rights

Supplier grants Customer the rights to use licensed software as defined in the Agreement.

Service level agreements and monitoring are not applicable to this type of service.

2.2 Maintenance and Support

Supplier provides its maintenance and support service description as defined in the Agreement.

Customer can choose the respective maintenance and support level based on it's assessment of the criticality of the respective Supplier function.

In case Suppliers defined support levels do not meet Customers' regulatory obligations, Customer and Supplier may agree on additional terms as required.

2.3 Professional Services

Customer and Supplier shall agree on applicable Service Level Agreements and its monitoring to support regulatory compliance in the respective professional services offering.

3 Subcontracting

3.1 In General

I. Supplier may, in its discretion, use service providers in the performance of its obligations under the Agreement.

II. In such case Supplier will conduct appropriate due diligence of the service provider before entering in any sub-contracting agreement.

III. Supplier will be responsible for the acts or omissions of its service providers which cause Supplier to breach any of its obligations under the Agreement.

IV. Upon Customer request, the Supplier shall provide Customer with sufficient information about applicable sub-contracting arrangements of the Supplier to enable Customer to meet its obligations to ensure supply chain security pursuant to the regulation and as determined by Customer in its discretion.

3.2 Subprocessors.

I. Notwithstanding the foregoing, Supplier's use of Sub processors will be exclusively governed by the terms of the relevant Data Processing Agreement between the parties.

II. Upon Customers request, the Supplier shall provide Customer with sufficient information about any sub processing arrangements of the Supplier to enable Customer to meet its obligations to ensure supply chain security pursuant to its regulatory obligations.

4 Locations

I. Upon Customer's request, Supplier shall certify in writing to Customer the locations at which the Customer's data is stored and the locations from which it provides the services in scope of the Agreement.

II. Supplier shall not implement any change to the above locations prior to informing Customer of such changes.

5 Supplier Security Policies and Controls.

I. Supplier will implement reasonable and appropriate measures designed to secure Customer Data against accidental or unlawful loss, access or disclosure in accordance with the Security Documentation.

II. The Supplier will maintain policies that ensure accessibility, availability, confidentiality, and integrity of all information assets related to the delivery of Software and/or associated services to Customers and apply risk management processes to guarantee to interested parties that information security risks are managed.

III. The policies and controls consist of specific requirements for asset management, access control, encryption, physical and environmental security, operations security, communication, Supplier management and data privacy.

IV. These policies have been defined, approved by management, published, and communicated to employees and relevant external parties in confidentiality.

5.1 Technical Organizational Measures

I. Supplier will ensure that its Software and/or associated services will comply to its security compliance standards comparable to ISO/IEC 27001 for the establishment, implementation, control, and improvement of the Software and/or associated services security standards. The applicable Technical and Organizational Measures are available here: www.softwareag.com/dpa-toms.

II. The Supplier shall continuously review its security and compliance standards and adapt them as necessary in order to ensure state-of-the-art protection.

5.2 Security Awareness and Training

I. Supplier has implemented a Global Information Security Awareness Program which includes regular mandatory **training** for all employees and additional measures to make them aware of constantly increasing Cyber Security Threats.

II. On request, Supplier will provide details about its program to Customer for the purpose of assessing adequate comparable level of its regulatory training requirements. In the event of significant gaps identified by Customer, Customer and Supplier shall agree in good faith on the improvements needed.

III. For Suppliers' professional services staff which support Customers' ICT environment, required awareness measures shall be agreed in the respective professional services offering.

5.3 Information Security Continuity

I. Supplier is responsible for ensuring operational resilience for its services to function under circumstances of disruptive events with minimal disruption to the service and minimize the effect of such an event to manage information security.

II. Supplier will maintain and regularly test business continuity planning and disaster recovery programs that are designed to minimize disruptions to its Software and/or associated services at least on an annual basis.

III. These tests include at a minimum vulnerability assessments and scans, open-source analyses, network security assessments, software scanning, source code reviews, compatibility testing, performance testing, end-to-end testing and penetration testing for the underlying infrastructure.

IV. Supplier will maintain its Business Continuity Management System and externally validate its respective ISO 22301 certification for scoped services.

V. For critical or important services Customer may request to be agreed as a separate service at additional cost:
   a. participation in its business resilience testing;
   b. have full access to relevant applicable documentation;
   c. dedicated Supplier contact to review and coordinate relevant activities.

5.4 Security Incident Response

I. In line with industry best practices Supplier shall maintain its information security incident response policy and procedures for the identification, analysis, containment, eradication, and post-mortem of security incidents related to the services in scope of the Agreement.

II. Any security incident that might affect the confidentiality, availability and integrity of Customer Data will be handled in accordance with the Supplier's Security Incident Management Policy.

III. Customer will be notified in alignment with Suppliers Support Incident SLA via the Customer Support Portal.

IV. If personal data is affected by the incident the Supplier shall notify Customers' data subjects without undue delay.

V. Supplier shall assist Customer in resolution of an incident related to services provided and at cause of Supplier at no additional cost and in alignment of Customer's regulatory obligations.

5.5 Vulnerability Management

I. Supplier will maintain a security vulnerability management program which manages vulnerabilities based on risk.

II. The software development process of Supplier includes regular static code analysis and code reviews.

III. As part of the vulnerability management process, vulnerabilities identified during security assessments will be addressed in a timely manner, based on criticality.

5.6 Penetration testing

I. Application Penetration Testing is an obligation of Customer and is not relevant to Supplier which provides uses rights to the Customer for using its software to develop business applications and operates them in their IT infrastructure.

II. Upon Customer request the Supplier shall support its Threat Led Application penetration testing activities for critical or important services to be agreed as a separate service at additional cost.

III. Our corporate IT infrastructure is subject to regular internal and external penetration testing.

6 Reporting and Information Obligation

For Critical or Important Services, Supplier shall report to the Customer any developments that could have a material impact on its ability to effectively deliver its services in accordance with the agreed performance levels.

Customer may request to be agreed as a separate service at additional cost

I. Supplier to regularly provide the Customer with appropriate reports on its activities and services.

II. Reports on incidents, including operational security incidents and business continuity measures and tests.

7 Monitoring of Services

For critical or important functions, Customer and Supplier shall cooperate to ensure that status of service monitoring is kept up to date for defined SLA as defined in any respective service descriptions.

Upon Customer request and to be agreed as a separate service at additional cost the Supplier shall

I. provide information to the Customer about its performance management regarding agreed SLA

II. implement any corrective actions necessary to correct any failures to meet or exceed service levels attributable to such Services, as agreed with Customer in good faith from time to time

III. inform Customers about material risk identified regarding availability, authenticity, integrity and confidentiality of Customer Data mapped.

IV. report on implemented measures regarding its security policies and standards.

8 Audit Rights

8.1 Cooperation with the competent authorities and the resolution authorities of Customer

I. Supplier shall fully cooperate with the competent authorities and the resolution authorities of Customer, including persons appointed by them, in connection with any investigation or other activity by the competent authorities and/or the resolution authorities concerning the Agreement or Customer, upon prior formal request by the respective competent authority or resolution authority, or where legally required upon prior written request by Customer.

II. If a Regulator makes a formal written request to Customer to access or examine any services within the scope of the Agreement, Customer will use all reasonable efforts to resolve the request directly with the Regulator using alternative methods, including by reference to and provision of the Security Documentation to the Regulator, discussing the request with Supplier subject matter experts, and affording the Regulator access to Customer Content through Customer's access credentials.

III. If the Regulator notifies Customer in writing that it requires additional information to verify compliance with applicable laws and regulations then, upon Customer's written request, Supplier will provide the Regulator with: (i) the opportunity to discuss any services within the scope of the Agreement with Supplier subject matter experts; and (ii)

if required by the Regulator, a direct right to examine any services within the scope of the Agreement used by Customer.

IV. Any direct examination of the Supplier facilities will be subject to Supplier's reasonable security and access requirements. Supplier may charge Customer, at Supplier's then current time and materials rates, for any such discussion, communication and examination.

V. The provisions of this Section relating to the Regulator's right to examine are not intended to conflict with or limit any applicable laws or regulations, and nothing in this section should be construed as an impediment to the exercise of the Regulator's lawful authority, including the right to examine any services within the scope of the Agreement.

8.2 Audits by Customer

I. In the event that Supplier receives a written request from Customer to assist in Customer's regulatory obligations relating to vendor examination, oversight, and audit requirements, Supplier will provide Customer with copies of the Customer facing Security Documentation, reasonable access to Supplier subject matter experts, and reasonable access to Supplier's relevant third-party external auditors.

II. The foregoing is designed to provide Customer with effectively the same access to information and personnel that Supplier would provide a Regulator, while preserving Supplier's ability to operate any services within the scope of the Agreement, and protect the privacy and confidentiality of other customers' data.

III. To request an audit, Customer must submit a detailed audit plan at least ninety (90) days in advance of the proposed audit date to Supplier describing the proposed scope, duration, and start date of the audit. Upon Customer request, Customer and Supplier may agree in written form on different audit notification periods.

IV. Supplier will review the audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Supplier's security, privacy, employment or other relevant policies).

V. In the event that Customer requires additional information from Supplier that is not satisfied by the above or not a result of a regulatory obligation, Supplier may provide such in Supplier's sole discretion and at Customer's sole cost and expense.