Security Compliance Attachment to DORA-Addendum

The SCA supports Customers in managing their ICT third-party risks according to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 Digital Operational Resilience Act (DORA) Clauses ("DORA").

1. Subcontracting

I. Supplier may, in its discretion, sub-contract Software and/or associated Services, including any services supporting critical or important functions of Customer to third parties (hereinafter "Sub-Processors"). Any Sub-Processors that are affiliated to Supplier shall not be subject to the provisions of this Section.

II. Upon Customer request, the Supplier shall provide Customer with sufficient information about applicable sub-processing arrangements of the Supplier to the extent that Customer requires such information to meet its statutory obligations.

III. For any services supporting critical or important functions of the Customer, the following shall apply:

1. Supplier is responsible for the provision of the services provided by Sub-Processors and shall ensure continuity of the Software and/or associated Services throughout the chain of Sub-Processors. Supplier shall notify Customer of any material change to a relevant sub-processing arrangement within 30 days prior to such change. In case Customer does not object within such notice period, changes shall be implemented upon expiry of the notice period.

2. Supplier will conduct appropriate due diligence of Sub-Processors including the assessment of all risks associated with the location of the Sub-Processor, it's parent company and the location the services are provided from before entering into any sub-processing agreement.

3. Supplier shall monitor its' Sub-Processors accordingly and shall endeavor to contractually oblige its' Sub-Processors to

   i. report to Supplier any developments that could have a material impact on its ability to effectively deliver its services in accordance with the agreed performance levels;

   ii. implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the Customer in line with its regulatory framework;

   iii. grant Customer, relevant competent and resolution authorities materially the same audit rights as described under Section 7 of the SCA;

2. Locations

I. Locations, namely the regions or countries, where the Software and/or associated Services are provided and where data is processed, including the storage location, can be found in the applicable Sub-Processor list under: www.softwareag.com/technical-and-organisational-measures-toms-subprocessors.

II. Supplier shall not implement any change to the above Locations prior to informing Customer 30 days in advance of such changes.

3. Data Protection

I. Information on availability, authenticity, integrity and confidentiality in relation to the protection of data can be found in the Security Documentation (see 4.1.I).

II. The processing of personal data is governed by the applicable Data Processing Agreement.

4. Information Security

4.1 Security measures, tools and policies

I. The SCA is supplemented by Supplier's then current Security Documentation, as made generally available to Supplier's Customers from time to time under: www.softwareag.com/software-gmbh-security-compliance-attachment. Security Documentation is Supplier Confidential Information.

II. Supplier will ensure that idts Software and/or associated Services will comply to security compliance standards comparable to ISO/IEC 27001.

4.2 Information Security Continuity

I. Supplier is responsible for ensuring operational resilience for its Software and/or associated Services striving for continued availibility of Software and/or associated Services under circumstances of disruptive events and endeavoring to minimize any potential disruption.

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. 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.

III. Supplier will maintain its Business Continuity Management System and externally validate its respective ISO 22301 certification for Software and/or associated Services under the Agreement.

4.3 Security Incident Response

I. 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. Supplier shall maintain its Security Incident Management Policy and procedures for the identification, analysis, containment, eradication, and post-mortem of security incidents related to the Software and/or associated Services in scope of the Agreement.

II. In case of a security incident, including but not limited to a major operational incident, Customer will be notified in alignment with Supplier's Customer Support Incident SLA via the Customer Support Portal. In case of a major ICT-related incident, Supplier shall also notify competent authorities.

III. In case personal data is affected by the security incident the Supplier shall notify Customer in line with GDPR requirements.

IV. Supplier shall provide assistance to Customer when an incident related to the Software and/or associated Services provided occurs, provided that such incident is caused by Supplier. In all other cases, assistance to Customer shall be charged according to Supplier's then current Professional Services daily rates.

4.4 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 Security Awareness Program to Customer for the purpose of assessing adequacy regarding statutory requirements. In the event of significant gaps identified by Customer, Customer and Supplier shall agree in good faith on the improvements needed.

III. In case Supplier personnel is accessing Customer's network or ICT systems, such personnel shall reasonably participate in Customer's ICT security awareness program and digital operational resilience training. Any such participation shall be charged with Supplier's then current Professional Services daily rates. Customer and Supplier may agree that (i) only certain personnel, or types of personnel, participate in such training or (ii) an appropriate training is conducted by Supplier for its personnel. The Customer shall be reasonable in its request for Supplier's personnel to attend Customer's ICT security awareness programs and/or Digital Operational Resilience training, and acknowledges that it does not intend for such training to be excessive or unnecessary.

4.5 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.

4.6 Penetration testing

I. In case Software and/or associated Services are supporting critical or important functions of the Customer, the personnel that is accessing Customer's network or ICT systems, shall upon request of the Customer reasonably participate and fully cooperate in Customer's Threat Led Penetration Testing (TLPT). Any such participation shall be charged with Supplier's then current Professional Services daily rates. Customer and Supplier may agree that only certain personnel, or types of personnel, participate in such testing. The Customer shall be reasonable in its request for Supplier's personnel to attend Customer's TLPT, and acknowledges that it does not intend for such testing to be excessive or unnecessary.

II. Notwithstanding the foregoing, Supplier's corporate IT infrastructure is subject to regular internal and external penetration testing.

5. Reporting and Information Obligation

For Software and/or associated Services supporting critical or important functions, Supplier shall report to the Customer any developments within Supplier's or a relevant Sub-processor's sphere that could have a material impact on its ability to effectively deliver its Software and/or associated Services in accordance with the agreed performance levels.

As a separate service at additional cost, Customer may request

I. Supplier to regularly provide the Customer with appropriate reports on its activities and Software and/or associated Services.

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

III. Information on material risks identified regarding availability, authenticity, integrity, and confidentiality of Customer Data.

IV. Reports on implemented measures regarding Suppliers security policies and standards.

6. Monitoring of Software and/or associated Services

For critical or important functions, Customer and Supplier shall cooperate in defining measures and key indicators to monitor, on an ongoing basis, the performance of the Supplier, and the compliance of the Supplier with the Customer's policies and procedures.

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

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

7. Audit Rights

I. Customer has the right to monitor, on an ongoing basis, the Supplier's performance in respect of Software and/or associated Services supporting critical or important functions and measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, which entails the following:

1. Supplier grants unrestricted rights of access, inspection and audit, including ICT and threat-led penetration testing (together "Monitoring Measures") by the Customer, or an appointed third party, and by the competent authority (together "Inspectors"), and the right to take copies of relevant documentation on-site if they are critical to the operations of the Supplier. Any Monitoring Measures have to be requested in writing at least ninety (90) days in advance. Such request has to include a detailed audit plan with the proposed scope, duration and start date. Supplier will review the audit plan and provide Customer with any concerns or questions (e.g. in case any request compromises Supplier's security, privacy, employment or other relevant policies). Customer and Supplier may agree on different notification periods in writing.

2. In case other customers' rights are affected by such Monitoring Measures, Supplier may ask Inspectors prior to any Monitoring Measures to provide a detailed list of queries and document requests. In case the latter information requests can be satisfied in writing and /or via other means of communication, no further on-site Monitoring Measures shall be conducted. Supplier may anonymize and redact other customers' information in advance.

3. Notwithstanding the foregoing, Customer may use the following Monitoring Measures, where appropriate,

   a. its own internal audit or an audit by an appointed third party;

   b. pooled Monitoring Measures, that are organized jointly with other contracting financial entities or firms that use ICT services of the Supplier;

c. third-party certifications;

d. internal or third-party audit reports made available by the Supplier.

II. Any Monitoring Measures/Audits are subject to Supplier's reasonable security and access requirements as well as reasonable access to Supplier subject matter experts and third-party external auditors.

III. Unless there is reason to assume serious breach of security and/or business continuity best practices, Monitoring Measures may not be conducted more than once during the Term of the Agreement.

IV. Supplier shall fully cooperate during the onsite Monitoring Measures performed by the Inspectors and/or the Lead Overseer.