Order Form

Software AG (Reg No. HRB 1562) of Uhlandstraße 12, D-64297 DARMSTADT ("**Software AG**") is the holder of distribution and/or exploitation rights relating to the cloud services set out in this Order Form (together hereinafter referred to as "**the Cloud Services**") which it has agreed to make available to your institution ("**Customer**") for research and education purposes only. The use by the Customer of the Cloud Services is governed by the terms and conditions set out in the Agreement referred to below together with any associated amendments thereto (collectively herein referred to as the "**Agreement**").Capitalized terms used in this Order Form but not otherwise defined herein will have the meanings given to them in the Agreement. In the event of any conflict between any provision of this Order Form and the Agreement, such conflict will be resolved by giving precedence to this Order Form. Any contrary or additional terms and conditions included in any purchase order or similar document (printed or online) related to this Order Form will be invalid and non-binding.

Cloud Services

Product Name and Operating System	Quantity and License Metric	Product Code
Cumulocity IoT Small 100 SaaS bundle on Hosted Software comprising:	1 X Each	IOBSB
- Cumulocity IoT Core Platform on Hosted Software	1 X Tenant	IOTBZ
- Cumulocity IoT Usage - Devices on Hosted Software	100 X Device pay per unit	IOTUD
- Cumulocity IoT Usage - Inbound Data Tra. on Hosted Software	20 X Inbound Data Transfers pay per unit	IOTUI
- Cumulocity IoT Usage - Data stored on Hosted Software	100 X Data Stored pay per unit	IOTUS

Cumulocity IoT SaaS Bundle - Cloud Service Information

General Information	The Cumulocity IoT Platform is a Platform for the Internet of Things to connect and manage devices as well as to visualize and analyze data delivered in a Software-as-a-Service model. The underlying infrastructure is hosted in Amazon Web Services (AWS). Supplier maintains, monitors and secures the shared architecture.
Cloud Delivery Model	Shared Environment - Single-Tenant
Cloud Deployment Model	Managed Cumulocity Cloud
Cloud Infrastructure Services	Hosted on Amazon Web Services (AWS) infrastructure in the selected Data Storage Location set out below. Base Operating Model: Linux Operating System. Base Amazon Web Services Components: EC2, EBS, VPC und S (For more details on the definition of these services, visit https://aws.amazon.com/)
Cloud Service Availability	99.90% based on Web Services availability measured over 5 minute intervals per calendar month (excluding standard scheduled maintenance).
Maintenance Window	As agreed between the parties from time to time
Cloud Data Storage Location	Frankfurt
Service Access Option	To use Cumulocity applications, you need a modern web browser. We test with the following desktop web browsers: - Edge Browser - Internet Explorer (latest version) - Firefox (latest version) - Chrome (latest version) You can also use recent smartphone and tablet web browsers. We test with the following mobile web browsers: - Chrome on Android (latest version) on Galaxy smartphones and tablets - Safari on iOS (latest version) on Apple iPhone and iPad Service is also accessible by REST APIs as described at http://www.cumulocity.com/guides/reference/rest-implementation/.
Cloud Data Backup	Frequency: Daily, 30 days retention Data Backup Location: Same Web Services region as the Data Storage Location referred to above but different Web Services availability zone
Emergency	Recovery Point Objective 24h based on daily backups Recovery Time Objective: 12h
Cloud Exit Terms	Access to the Cloud Services will be removed upon termination of the Agreement. Customer will be able to download a final backup of the Customer Data within 14 days' after termination of the Agreement (the "**Exit Period**"). After the Exit Period, Supplier will delete the Customer's environment/tenant and the Customer Data following industry-standard practices.
Features	Role-based access control Device management (Alarm-, Configuration-, Firmware-, Software- Management) Real-time analytics with smart rules Real-time data visualisation with custom dashboards Access to APIs, SDKs, development tools, documentation, etc. Unlimited users One Standard Tenant Active-Active Dr (Two Active Data Centers Sharing The Load)
Cloud Services Term	90 days from the date of this Agreement
Cloud Services Delivery Entity	Cumulocity GmbH Reg. No. HRB 68832 (AG Düsseldorf); registered office: Speditionstraße 13 40221 Düsseldorf, Germany

License Metrics

Device pay per unit	A "Device" means any asset, including but not limited to physical units of hardware, that is sending or receiving data which is managed by the Software (connected Device). Any connected Device has an own ID number that is reported over APIs and registered in the device management application. The licensed quantity is measured in Devices per month.
Inbound Data Transfers pay per unit	Use by the Customer of the Cloud Services whose Usage Metric is indicated as 'Inbound Data Transfers' above is limited to use only in respect of a number of inbound data

	transfers which do not exceed, in aggregate, the licensed number indicated above. Inbound Data Transfers refers to the total number of inbound data transfers recorded using Cumulocity's IoT platform's REST and MQTT interfaces. The creation along with each update of a "data entry" is counted as an IDT unit. A "data entry" can be a measurement, alarm, event or inventory object. Operations are not counted as IDT units. Inbound requests usually come from a device but can also originate from a custom microservice, website or any other client. When sending bulk requests containing multiple data entries (e.g. measurements), each data entry will be counted individually. The licensed volume is measured in units of 100,000 Inbound Data Transfers.
Data Stored pay per unit	Total volume of data that is stored on the infrastructure provided by the Supplier. The licensed volume is measured in Units of 100 MB per month.
Each	Use by the Customer of the Cloud Service functionality whose License Metric is indicated as 'Each' above is limited to the installation and use by the Customer of the licensed number of copies of the same referred to above.
Tenant	A dedicated share of a Cloud Services installation instance including its own logical database, configuration, user management and other individual functionality for the Tenant. A Tenant is accessible with a unique URL.

1 USE OF SERVICES

1.1 **Provision of Cloud Services**: Subject to the terms and conditions set forth in this Agreement and in exchange for payment of the Cloud Services Fee, the Supplier grants the Customer a temporary, non-exclusive, non-transferable right to access and use the Cloud Services subject to the terms of this Agreement on a separate Tenant installation for the duration of the Cloud Services Term and to connect Devices to the Cloud Services; and use the Cloud Services for the processing of data via Inbound Data Transfers.

2 OBLIGATIONS

2.1 **Customer's Obligations**: During the Cloud Services Term, Customer shall have the following obligations:

(a) The Customer is solely responsible for providing connectivity between Devices and the Cloud Services.

(b) The Customer shall inform Supplier if any dispute arises in respect of the Cloud Services and to comply with all reasonable instructions of Supplier in relation thereto.

(c) The Customer agrees to include in all Cloud Services or Professional Services communication and documentation the trademark and copyright notices of Supplier. Customer is obliged to submit all of its materials containing Supplier trademarks to Supplier for prior approval. Approval shall only be given where, in Supplier opinion, use is appropriate to the Supplier market image and status. Customer remains fully responsible for such materials and their content as well as compliance with applicable law.

(d) The Customer agrees that Supplier can use the Customer name, logo and use case on the Supplier website, materials and presentations. Supplier agrees to follow any Customer brand guidelines that it is aware of, related to presenting the Customer name and logo in its materials.

(e) The Customer is solely responsible for all Customer data provided to Supplier or uploaded to, stored in or transmitted through the Cloud Services and the use of the Cloud Services. Such responsibility shall include (but not be limited to) securing any privacy-related rights and permissions as may be required by local law or by the Customer's internal policies and making backup copies in order to prevent any loss or damages.

(f) The Customer warrants and represents that it shall maintain security measures covering, without limitation, confidentiality, authenticity and integrity to ensure that the access to the Cloud Services granted under this Agreement is limited as set out under this Agreement.

(g) In order to access and use the Cloud Services, the Customer will need to register and create user accounts within a Tenant surrounding. To create an account the Customer is required to provide certain personal information about the registrant and create a user name and password ("Account Information"). The Customer agrees to provide accurate, current and complete Account Information. Supplier reserves the right to suspend or terminate any account or Tenant if any Account Information provided during the registration process or thereafter is or becomes inaccurate, false or misleading. The Customer is responsible for maintaining the confidentiality of its Account Information and agrees to notify Supplier if its Account Information is lost, stolen, or disclosed to an unauthorized third party, or otherwise may have become compromised. The Customer is responsible for all activities under its account.

Effective Date
The date on which the Customer first access the Cloud Services

CLOUD SERVICES TERMS AND CONDITIONS

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 HAVE AUTHORITY TO ACT ON BEHALF OF YOUR INSTITUTION ("**CUSTOMER**") IN DEALING WITH THE RELEVANT SOFTWARE AG GROUP COMPANY ("**SUPPLIER**")

1 USE OF SERVICES

1.1 **Provision of Cloud Services**: Supplier grants Customer a non-exclusive, non-transferable, non-sublicensable right to access and use 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 research and education purposes only and not further or otherwise. Customer will not receive a copy of any programs listed in the Order Form other than for temporary download of plug-ins or fat clients (which will be deemed part of the Cloud Services) as described in the applicable Order Form. "**Users**" of the Cloud Services mean employees or contractors of Customer or students engaged in studying at eh 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 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.

1.2 **Restrictions**: Customer will comply with all laws and regulations applicable to Customer and to Customer's use of the Cloud Services. Customer will not, or permit or cause any third party to:

(a) use the Cloud Services other than expressly authorized by, and in accordance with the usage terms of, this Agreement;
(b) license, sub-license, sell, rent, lease, transfer, assign, distribute, outsource, permit time sharing or service bureau use, or otherwise commercially exploit or make the Cloud Services available to any third party, other than as expressly permitted by this Agreement and by international export laws and regulations;
(c) disassemble, reverse engineer, reverse compile, translate, modify, adapt, alter, copy or create derivative works from any products or services provided with the Cloud Services except to the extent permitted by applicable law;
(d) interfere with or disrupt the integrity or performance of the Cloud Services or the data contained therein in any way, including but not limited to: (i) conducting penetration testing in multi-tenant environments; (ii) conducting penetration tests in single-tenant environments without the Supplier's prior written consent; (iii) attempting to gain unauthorized access to the Cloud Services or their related systems or networks; or (iv) storing or transmitting a virus or other malicious code through the Cloud Services;
(e) disseminate performance-related information relating to the Cloud Services;
(f) use the Cloud Services to store or transmit infringing, libelous, offensive, unlawful or tortious material; or
(g) store or process any personal data of the following types: information on a person's racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health (HITECH - Health Information Technology for Economic and Clinical Health Act & HIPAA - Health Insurance Portability and Accountability Act), sex life, concerning bank or credit card accounts (PCI DSS - Payment Card Industry Data Security Standard) comprising but not limited to data according to GDPR Art. 9 No. 1;

1.3 **Service Level**: Supplier will use commercially reasonable efforts to make the Cloud Services accessible to Customer, subject to the availability of third party infrastructure, required and emergency maintenance, availability of third party networks and communications facilities and force majeure events. The Cloud Services are hosted on a shared third-party infrastructure environment as set forth in the applicable Order Form.

1.4 **Reservation of Rights**: Supplier owns all intellectual property rights in and to the Cloud Services, Documentation and all related materials and derivative works thereof. There is no transfer or assignment by Supplier of any ownership right and Supplier reserves all rights not expressly granted under this Agreement.

2 CUSTOMER INFORMATION

2.1 **Operational Data; Feedback**: Supplier will automatically collect information associated with Customer's access and use of the Cloud Services, including, without limitation application telemetry, IP addresses, IP configurations, stored sessions, open ports, Credentials, network metadata, and device operating system, status, version and configuration (collectively "**Operational Data**"). Supplier may use the Operational Data to monitor, analyze, develop, support or improve the performance of the Cloud Services. Customer grants to Supplier a worldwide, perpetual, irrevocable license to use and commercialize any suggestions, enhancement, requests, recommendations, corrections or other feedback provided by Customer relating to the Cloud Services.

2.2 **Customer Data**: With the exception of Operational Data, Customer owns all content, information, materials and intellectual property provided by Customer in connection with Customer's use of the Cloud Services ("**Customer Data**"). Customer is solely responsible for: (i) its provision and use of Customer Data with the Cloud Services; (ii) the accuracy, quality and content of the Customer Data; (iii) assessing the Cloud Services suitability for Customer's intended use; and (iv) obtaining all necessary rights, consents and permissions. Customer will comply with all applicable laws, in its provision and use of Customer Data in connection with the Cloud Services. Customer grants Supplier a worldwide, irrevocable, non-transferable, non-assignable (except as permitted under this Agreement), sub-licensable, non-exclusive license to access, retrieve, store, copy, display, distribute, transmit and otherwise use Customer Data associated with the Cloud Services as follows:

(a) in connection with maintaining, providing and/or making available the Cloud Services; and
(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.

2.3 **Data Protection 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**").

2.4 **Cloud Services Privacy Policy**: Supplier will collect and process any Operational Data that qualifies as Personal Data in accordance with its then current Cloud Privacy Policy which is incorporated herein by this reference. Supplier reserves the right to change its Cloud Privacy Policy from time to time by posting a new version at https://www.softwareag.com/corporate/cloud_privacy_policy. Customer may subscribe to email notifications regarding new versions of the Cloud Privacy Policy. Customer agrees to and accepts any modified terms by continuing to use the Cloud Services after such changes are posted and effective.

2.5 **Security**: Supplier will maintain reasonable administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data. Supplier 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).

3 CONFIDENTIALITY

3.1 **Confidential Information**: Each Party will have access to confidential or nonpublic information ("**Confidential Information**") of the other Party or third parties. Confidential Information disclosed is proprietary and will remain the sole property of the disclosing Party or such third parties. The Cloud Services and Documentation are Confidential Information of Supplier. Confidential Information will not include information that: (i) is or becomes publicly available or enters the public domain through no fault of the recipient; (ii) is rightfully communicated to the recipient by persons not bound by confidentiality obligations; (iii) is already in the recipient's possession free of any confidentiality obligations at the time of disclosure; (iv) is independently developed by the recipient; or (v) is approved, in writing, for release or disclosure without restriction.

3.2 **Confidentiality Obligation**: Each Party agrees to: (i) use Confidential Information only for the purposes of this Agreement; (ii) hold Confidential Information in confidence and protect it from dissemination to, and use by, any third party; (iii) not to create any derivative work from Confidential

Information; (iv) restrict access to Confidential Information to its employees, affiliates, agents, and contractors who need access to such Confidential Information and who have agreed in writing to treat such Confidential Information in accordance with this Agreement; and (v) return or destroy all Confidential Information of the other Party upon termination or expiration of this Agreement. The recipient may make and retain copies of Confidential Information as required by law and/or regulatory requirement, or that are automatically stored by backup systems and which are not accessible in the normal course of business. If the recipient is required by law or valid legal order to disclose Confidential Information, the recipient will, unless prohibited by law, give reasonable notice of such demand to allow the disclosing Party to seek a protective order or other remedy.

4 WARRANTY DISCLAIMER

4.1 **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 PARTICULAR PURPOSE.

5 IPR INDEMNITY

5.1 **Indemnity**: Supplier shall indemnify, defend, and hold Customer harmless from any action brought by a third-party against Customer to the extent that it is proximately caused by an allegation that the Cloud Services provided under this Agreement have infringed an intellectual property right or trade secret registered in the country of Supplier´s residence, and pay those damages or costs related to the settlement of such action or finally awarded against Customer in such action, including but not limited to reasonable attorneys' fees, provided that Customer:

(a) promptly notifies Supplier of any such action; and
(b) gives Supplier full authority, information, and assistance to defend such claim; and
(c) gives Supplier sole control of the defense of such claim and all negotiations for the compromise or settlement of such claim.

5.2 **Exceptions**: Supplier will have no indemnity obligation nor other liability under this Agreement to the extent the claim is based upon: (i) Cloud Services modified by anyone other than Supplier; (ii) use of other than the then-current release of any fat clients or plug-ins provided to Customer for the purposes of accessing and using the Cloud Services, if the infringement could have been avoided by use of the then-current release and such current release has been made available to Customer; or (iii) use of the Cloud Services in conjunction with other software, hardware or Customer data, where such use gave rise to the infringement claim.

5.3 **Remedy**: If Supplier determines that the Cloud Services are likely to be the subject of a claim of infringement, Supplier may, in its sole discretion: (i) replace or modify the Cloud Services; (ii) procure the right for Customer to continue using the Cloud Services; or (iii) terminate access to the Cloud Services and refund to Customer a pro-rated portion of the applicable unused Cloud Services fees. THIS SECTION STATES SUPPLIER'S EXCLUSIVE LIABILITY AND CUSTOMER'S EXCLUSIVE REMEDY REGARDING ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT BY THE CLOUD SERVICES OR ANY MATERIALS OR SERVICES PROVIDED UNDER THIS AGREEMENT.

5.4 **Customer Indemnity**: Customer will indemnify Supplier from any third party action against Supplier to the extent proximately based upon an allegation arising from: (i) any access to or use of Customer Data with the Cloud Services; or (ii) modification or use of the Cloud Services with any Customer applications, provided that Supplier (a) promptly notifies Customer of any such action; (b) gives Customer full authority, information, and assistance to defend such claim; and (c) gives Customer sole control of the defense of such claim and all negotiations for the compromise or settlement of such claim.

6 LIMITATION OF LIABILITY

6.1 **Limitation of Liabilty**: To the extent permitted by law, Supplier shall not be liable for any damages caused by the use of the Cloud Services.

7 USAGE LIMITS

7.1 **Usage Limits**: Customer will ensure that is usage of the Cloud Services does not exceed the usage terms set forth in this Agreement and will be liable for any excess usage at Supplier's then current rates during the period in which usages exceeds the licensed amount.

8 TERMINATION

8.1 **Termination:** The Customer's right to use the Cloud Services will automatically terminate as of the date set forth in this Agreement or, if not otherwise specified herein, thirty (30) days after the date that the Customer is first permitted access to the Cloud Services by the Supplier. Notwithstanding the foregoing, Supplier may immediately terminate the Agreement upon written notice to the Customer. Upon any termination (howsoever arising) or expiry, the Customer shall cease using the Cloud Services. If requested by Supplier, the Customer shall send a letter certifying that the provisions of this clause have been adhered to. All disclaimers of warranties, limitations of liability and provisions for the protection of Supplier's proprietary rights in the Cloud Services as set forth herein shall survive any termination of the Agreement.

9 GENERAL

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

9.2 **Governing Law**: This Agreement is governed by the laws of Germany without giving effect to its conflicts-of-laws provisions and excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG). The parties consent and submit to exclusive personal jurisdiction, procedure and venue for legal disputes arising from or connected with this Agreement shall lie with the courts of Darmstadt, Germany. Arbitration processes are excluded.

9.3 **Entire Agreement; Waiver; Priority; Severability**: This Agreement constitutes the entire agreement between the Parties, and supersedes all prior written and oral agreements and communications related to the subject matter of this Agreement. Any modifications to this Agreement must be in writing and signed by the duly authorized representatives of the Parties. Any waiver under this Agreement must be in writing and signed by the Party granting the waiver. A waiver granted under this Agreement will not be deemed to be a waiver of any subsequent breach of the same or any other provision of this Agreement. No failure or delay by either Party in exercising any right under this Agreement will constitute a waiver of that right. In the event of any conflict between any provision of this Agreement and any exhibits incorporated and made part of this Agreement, such conflict will be resolved by giving precedence to the Order Form(s). Any contrary or additional terms and conditions included in any purchase order or similar document (printed or online) related to this Agreement will be invalid and non-binding, even if received, accepted, approved, or signed by a Party. If any provision of this Agreement is held invalid or unenforceable, the provision will be limited to the minimum effect necessary and the remaining provisions of this Agreement will remain binding and enforceable. This Agreement may be executed in one or more counterparts, with the same effect as if the Parties had signed the same document. The Parties agree to the use of digital signatures.

PRIVACY POLICY FOR CLOUD & MANAGED SERVICES

This Privacy Policy covers the privacy practices of the Supplier with effect from 1st September 2018 in relation to the use of the Cloud Services ("**Services**") by the Customer.

1 INFORMATION COLLECTED

1.1 **Collected Data**: The Supplier may collect and process Personal Data (within the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**") in connection with Customer's access and use of the Services.

1.2 **Scope**: This Privacy Policy does only apply to Personal Data that is collected by the Supplier in its role as data controller in order for the Cloud Services to perform the function for which they are designed. For any Personal Data that is processed by the Supplier in its role as data processor on behalf of the Customer, the Data Processing Agreement entered into between Customer and Supplier shall apply. Any Personal Data that is processed within the Cloud Services for purposes and means determined by the Customer (e.g. Personal Data of the Customer's customers/employees/officers/etc.) is being processed on behalf of the Customer.

1.3 **Categories of Data**: The data the Supplier is collecting and processing in its role as data controller comprises the following categories of Personal Data:

(a) first name, last name, email address, country, job title, phone number, fax number, company name, used products of the Supplier and additional information provided when contacting the Supplier using the websites, especially information provided in free text fields of contact forms ("**contact data**");

(b) additional data provided to the Supplier in comments on the Supplier websites, especially in forms of discussion boards and using the comment features of blogs ("**comment data**");

(c) Personal Data sent by the User's web browser, i.e. information about the type of web browser, the operating system and selected settings (e.g. language, region, font size, font types and other configuration) may be collected ("**browser data**");

(d) IP address, information about the amount of data transferred, stored in access log files ("**usage data**").

2 PURPOSES AND LAWFULNESS OF THE DATA PROCESSING

2.1 **Purposes**: The Supplier collects, processes, and uses Personal Data to the extent required to fulfill the respective purposes:

(a) **Providing the Services**: In accordance with the terms and conditions of the Cloud Services Agreement, the Supplier collects processes and uses Personal Data for the purpose of providing the Services, preventing or addressing service or technical problems, in connection with a Customer support matter, for billing, customization, training or as may be required by law. The lawfulness for the data processing is the performance of a contract (the Cloud Services Agreement). Using this Personal Data is required to provide the contractual obligations. Without this Personal Data it would be not possible to receive the Services offered by the Supplier.

(b) **Security Purposes**: The Supplier will also use usage data for internal system-specific purposes to secure the websites and IT systems from malicious attacks by third parties. The lawfulness is a balancing of interests of the conflicting interests of the security of the IT systems on the Supplier's part and the Customer's potentially conflicting interests in a non-processing of the usage data by the Supplier. Taking into account the security and organizational measures of the processing of the usage data by the Supplier, the Supplier considers Customer rights and interests appropriately taken into account and protected.

(c) **Marketing Purposes**: In so far that consent has been given, the Supplier will also use Personal Data for marketing purposes, e.g. to send newsletters. The lawfulness for processing this data is the Supplier's legitimate interest, e.g. to improve the Services, or consent.

(d) **Improvement:** In so far that consent has been given, the Supplier will also use browser data for market research and the improvement of its Services, and to improve the user experience. The lawfulness for processing this data is consent or the Supplier's legitimate interest.

(e) **Statistical Purposes**: In so far that consent has been given, the Supplier will also collect usage data for statistical purposes, for the analysis of advertisement on its websites, and for adapting the advertisement for its products and services to better match the users' interests. Log files are only used for statistical analysis of the visitors of the Supplier websites. The data is deleted after having been analyzed. The lawfulness for processing this data for statistical purposes is the Supplier's legitimate interest, e.g. internal organization, or consent.

Providing direct marketing data and browser data is optional. If such data is not provided, no direct marketing information will be sent and Personal Data will not be used to improve the user experience and will not be used for statistical purposes.
Beyond these purposes, the Supplier uses and processes Personal Data only if prior consent has been expressly granted thereto and if information about the purposes has been provided. In particular, the Supplier does not use Personal Data for automated individual decisions and profiling.

3 DATA RECIPIENTS

3.1 **Supplier's Departments**: Personal Data will be processed by employees/officers/agents of the Supplier in the respective departments who need to know the Personal Data for the respective purposes.

(a) contact data: any departments that might be involved to process a Customer request; marketing and sales departments responsible for the Customer's region

(b) comment data: marketing or the respective product departments that are responsible for operating the blogs or discussion boards

(c) browser data and usage data: marketing and the IT departments that are responsible for operating the respective websites

3.2 **External Service Providers**: The Supplier has contracted external data processing service providers to collect and process Personal Data on behalf and according to the instructions of the Supplier. Such service providers support the Supplier, especially relating to administering, hosting, distributing, reselling, and/or supporting the Services, hosting and operating the websites and blogs, marketing purposes, statistical analysis, improving the websites and sending Supplier's email newsletters. If these external companies have access to Personal Data, respective data processing agreements are in place. The entity hosting the Services ("**Hosting Entity**") is identified in the Cloud Services Attachment or other contract document between the Supplier and the Customer.

3.3 **External Service Providers outside the EU/EEA**: The service providers may be located outside the European Union or the European Economic Area. The Supplier is a globally operating corporation. In order to better process the Customer's matter, it might be also necessary to forward data to local subsidiaries or to local distribution partners, whose registered office might also be located in countries outside the European Union or the European Economic Area. Such data transfers take place within the Supplier's group companies and the service providers listed in Appendix 1 only for the aforementioned purposes. The lawfulness of the data export is the Supplier's legitimate interest or legitimate interests of the recipients, e.g. internal administrative purposes, and no higher legitimate Customer interests, the fulfillment of legal obligations or consent.

Beyond that, the Supplier does not forward Personal Data to other third parties, unless the Supplier is obliged to do so by virtue of statutory provisions or order of any judicial or other public authorities or consent has explicitly been given for that purpose. In particular, Personal Data will not be sold, leased or exchanged.

4 DATA TRANSFERS TO THIRD COUNTRIES

4.1 **Data Transfers to Third Countries**: The recipients of Personal Data might be located outside the European Union or the European Economic Area and therefore might not have a data protection equivalent to EU data protection law.
Unless there is an adequacy decision by the EU Commission for these states or the transfer is based on an exemption provided for by the GDPR (e.g. express consent, assertion, exercise or defense of legal rights), the Supplier will take all necessary measures to ensure that transfers to such organizations are adequately protected, e.g. by signing the standard contractual clauses stipulated by the EU Commission ("**SSC**") with the data recipients or be relying on Privacy Shield Principles ("**PSP**"). A copy of these reasonable warranties may be requested by contacting the Supplier's Data Protection Department at: dataprotection@softwareag.com.
A transfer of data to official authorities in countries outside the European Union or the European Economic Area (so-called third countries) takes place, if required by law, express consent has been given or this is legitimated by the legitimate interest of the Supplier or the third party for data protection purposes, e.g. internal administrative purposes and no higher legitimate interests by Customer.

5 COMPLIANCE WITH PRIVACY SHIELD FRAMEWORKS

5.1 **Compliance with Privacy Shield Frameworks**: If Supplier transfers Personal Data from the EU and/or Switzerland to the U.S., respectively, the Supplier relies either on the EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Principles and/or in some cases standard contractual clauses have been signed. It is marked in Appendix 1 for which transfers the Supplier relies on EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Principles and for which standard contractual clauses have been signed. 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).
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 the Supplier's certification, please visit https://www.privacyshield.gov/.

6 RETENTION

6.1 **Retention**: Personal Data will be kept by the Supplier as long as necessary to provide the Customer with the requested Services. If the Supplier no longer needs the Customer's Personal Data to comply with contractual or legal obligations, they will be deleted from the systems or anonymized accordingly, so that identification is not possible, unless the Supplier has to keep the information, including Personal Data, to comply with legal or regulatory obligations (e.g. statutory retention periods which may arise from the commercial laws or tax laws and may in principle be 6 to 10 years or, if during the statutory limitation periods, which are regularly 3 years, but may be up to 30 years, evidence must be secured).

7 SECURITY

7.1 **Security**: The Supplier implements the technical and organizational measures that are commercially reasonable in relation to the respective purpose of data protection, in order to protect the information provided by the Customer against abuse and loss. Such data is stored in a secure operating environment that is not accessible to the public. In addition, each of the Supplier's employees is instructed on data protection and obliged to enter into a confidentiality agreement.

8 INFORMATION TRACKING

8.1 **Information Tracking**: Information about the usage of cookies, especially for marketing purposes, can be found in the Cookie Policy.

9 DATA SUBJECT RIGHTS

9.1 **Data Subject Rights**: Under applicable law, the Data Subject has the right under certain circumstances to
(a) request information about the stored Personal Data,
(b) rectification of Personal Data,
(c) restriction of processing of Personal Data,
(d) deletion of Personal Data,
(e) data portability,
(f) revocation of consent for processing of Personal Data and
(g) object to the processing of Personal Data.
Further information on the individual rights can be found in Appendix 2 to this Privacy Policy.
To exercise these rights and/or to address any questions, comments, or complaints regarding this Privacy Policy or the privacy practices of the Supplier, please contact the Supplier's Data Protection Department at:

Software AG
Data Protection Officer
Uhlandstraße 12
64297 Darmstadt
Germany
Email: dataprotection@softwareag.com

It is possible to send encrypted emails using S/MIME:
• X.509 certificate (zip file, contains dataprotection.cer)
• Software AG root certificate (zip file, contains SoftwareAGInternalCa2.cer).

The Data Subject also has the right to file a complaint with a data protection supervisory authority.

Additionally, 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 privacy and the collection or use of personal information. European Union and Swiss individuals with inquiries or complaints regarding this privacy policy should first contact the Data Protection Officer at the contact details mentioned above.
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 the Data Subject does not receive timely acknowledgment of his/her complaint, or if the 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, the Data Subject 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 the local Data Protection Authority. The Supplier is subject to the investigatory and enforcement powers of the United States Federal Trade Commission.

Appendix 1

Data Recipients in Third Countries

The following organizations in third countries could get access to Personal Data in certain cases. It has been ensured that these organizations provide an adequate level of data protection according to the General Data Protection Regulation ("**GDPR**") either by relying on the EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Principles ("**PSP**") and/or in some cases additionally standard contractual clauses ("**SCC**") have been signed.

#	Country	Name	Address	Legal Mechanism	
1	Australia	Software AG Australia Pty Ltd.	201 Miller Street, Level 16 North Sydney, NSW 2060	SSC	
2	Australia	Software AG Cloud APJ PTY Ltd.	Level 16, 201 Miller Street North Sydney, NSW 2060	SSC	
3	Bahrain	Software AG (Gulf) S.P.C.	Office No. 31, 3rd Floor, Building No. 1269, Road No. 3227, Block 332 Manama	SSC	
4	Brazil	Software AG Brasil Informatica e Serviços Ltda	Av. das Nações Unidas 12.901, 33° andar, Torre Norte CEP 04578-000 São Paulo/SP	SSC	
5	Chile	Software AG Factoria S.A.	La Concepción 141, Piso 8, Oficina 808, Santiago de Chile, CP8320176	SSC	
6	China	Software AG Limited	Room 1701-2, 17/F, No. 8 Fleming Road, Wanchai, HongKong	SSC	
7	India	Software AG Chennai Development Center India Pvt Ltd	VBC Solitaire, 4th Floor, No. 47 & 49, Bazulla Road, T. Nagar 600 017 Chennai	SSC	
8	India	Software AG Bangalore Technologies Private Ltd.	Embassy Tech Village 5th and 6th Floor, 2A East Tower, Marathahalli Outer Ring Road 560 103 Devarabisanahalli Bangalore	SSC	
9	Japan	Software AG Ltd. Japan	AKASAKA K-Tower 4F, 1-2-7 Motoakasaka 107-0051 Minato-ku, Tokyo	SSC	
10	Malaysia	Software AG Operations Malaysia Sdn Bhd.	Suite 2B-22-1, Level 22, Block 2B, Plaza Sentral, Jalan Stesen Sentral 5, Kuala Lumpur Sentral, 50470 Kuala Lumpur	SSC	
11	Mexico	Software AG, S.A. de C.V.	Blvd Manuel Avila Camacho No. 88 Piso 11, Torre Picasso, Col. Lomas de Chapultepec 11590 Mexico, Distrito Federal	SSC	
12	Philippines	Software AG, Inc.	12F Multinational Bancorporation Centre, Ayala Avenue, 1225 Makati City	SSC	
13	Russia	Limited Liability Company Software AG	Kosmodamianskaya Naberezhnaya, 52, building 4, 3rd floor, 115054 Moscow	SSC	
14	Singapore	Software AG Pte LTD	12 Marina Boulevard #17-04, Marina Bay Financial Centre Tower 3, 018982 Singapore	SSC	
15	South Africa	Software AG South Africa (Pty) Ltd	Culross on Main Office Park, 34 Culross Road, Building 3, 2021 Bryanston	SSC	
16	Turkey	Software AG Bilgi Sistemleri Ticaret A.S.	Degirmen Yolu Sok. No: 4, Sasmaz Plaza Kat: 9, TR-34742 Istanbul	SSC	
17	United Arab Emirates	Software AG International FZ-LLC	Star Building, EIB 4, Office # 204, P.O. Box # 502274, Dubai	SSC	
18	USA	Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109	SSC	PSP
19	USA	Software AG Cloud Americas, Inc.	1209 Orange Street Wilmington , DE 19801	SSC	PSP
20	USA	Software AG	11700 Plaza America Drive, Suite 700	SSC	

		Government Solutions, Inc.	Reston, VA 20190		
21	USA	Software AG USA, Inc.	11700 Plaza America Drive, Suite 700 Reston, VA 20190	SSC	PSP

Appendix 2

DATA SUBJECT RIGHTS

Under applicable law, the Data Subject has the right under certain circumstances to (1) request information about stored Personal Data, (2) rectification of Personal Data, (3) restriction of processing of Personal Data, (4) deletion of Personal Data, (5) data portability, (6) revocation of consent for processing of Personal Data and (7) object to the processing of Personal Data. In Detail this is:

1 **Right to information**: The Data Subject may have the right to ask the Supplier for confirmation of the processing of Personal Data in question and, if so, of the right to information about such Personal Data. The right to information includes, among other things, the processing purposes, the categories of Personal Data being processed and the recipients or categories of recipients to whom the Personal Data is disclosed. The Data Subject may also have the right to receive a copy of the Personal Data that is the subject of the processing. However, this right is not unrestricted, as the rights of others may limit the Data Subject's right to receive a copy.

2 **Right to rectification**: The Data Subject may be entitled to request the correction of incorrect Personal Data concerning the Data Subject. In consideration of the purposes of processing, the Data Subject has the right to request the completion of incomplete Personal Data, including by means of a supplementary statement.

3 **Right to erasure ("Right to be forgotten")**: Under certain conditions, the Data Subject has the right to ask the Supplier to delete Personal Data.

4 **Right to restriction of processing**: Under certain circumstances, the Data Subject has the right to demand that the Supplier restricts the processing of Personal Data. In this case, the corresponding data will be marked and processed by the Supplier only for specific purposes.

5 **Right to data portability**: Under certain circumstances, the Data Subject has the right to receive the Personal Data relating to him/her that the Data Subject has provided to the Supplier in a structured, commonly used and machine-readable format and the Data Subject has the right to transfer that data to another person without obstruction by the Supplier.

6 **Right to revocation of consent**: If the Data Subject has given consent for some data processing activities, he/she may revoke such consent at any time with future effect. Such revocation shall not affect the lawfulness of the processing on the basis of the consent until the revocation.

7 **Right to object**: For reasons arising from the Data Subject's particular situation, he/she has the right to object to the processing of Personal Data relating to him/her on the basis of Art. 6(1f) GDPR (data processing based on legitimate interests). If the Data Subject objects, the Supplier will no longer process his/her Personal Data unless compelling legitimate grounds for processing that outweigh the Data Subject's interests, rights and freedoms can be established or the processing is for the purposes of asserting, exercising or defending legal claims.

SOFTWARE AG CLICK WRAP DATA PROCESSING AGREEMENT

YOU SHOULD READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE ACCESSING AND/OR USING ANY SERVICES SPECIFIED IN THE AGREEMENT OF WHICH THESE CLICKWRAP DATA PROCESSING TERMS AND CONDITIONS FORM A PART ("**SERVICES**"). THE ACCESS AND/OR USE BY YOU OF ANY SERVICES WILL INDICATE YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS AND YOUR CONSENT TO BE BOUND BY THEM TOGETHER WITH YOUR ACKNOWLEDGEMENT OF YOUR AUTHORITY TO DO SO IN YOUR OWN RIGHT OR ON BEHALF OF YOUR COMPANY ("**CONTROLLER**") AND WILL CREATE A LEGALLY BINDING CONTRACT BETWEEN THE CONTROLLER AND SOFTWARE AG REG. NO. HRB 1562 OF UHLANDSTRASSE 12, D-64297 DARMSTADT ACTING IN ITS OWN NAME AND ACTING IN THE NAME AND ON BEHALF OF THE PROCESSORS LISTED IN APPENDIX 4 (EACH A "**PROCESSOR**"). IF YOU DO NOT AGREE WITH THESE SOFTWARE AG CLICK WRAP DATA PROCESSING TERMS AND CONDITIONS, YOU SHOULD NOT PROCEED WITH THE ACCESS AND/OR USE OF THE SERVICES.

PREAMBLE

WHEREAS, under the Agreement concluded between the Supplier and the Customer, the Supplier agreed to provide the Customer with the services as further specified in the Agreement and in Appendix 2 to this DPA (the "**Services**");

WHEREAS, the Parties agree that the bundling of the Processors (as listed in Appendix 4) within this single DPA is only undertaken for efficiency purposes (i.e. to avoid a multitude of different contract documents) and shall result in legally separate DPAs between the Controller and each Processor as designated in Appendix 4 and shall not create any legal or other relationship whatsoever between the bundled Processors other than between the Controller and each Processor separately;

WHEREAS, in rendering the Services, Processor may from time to time be provided with, or have access to information of Controller's end-customers or to information of other individuals having a (potential) relationship with Controller and this information may qualify as personal data within the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**") and other applicable data protection laws;

WHEREAS, Controller engages Processor as a commissioned processor acting on behalf of Controller as stipulated in Art. 28 GDPR;

WHEREAS, European data protection laws require controllers in EU/EEA countries to provide adequate protection for transfers of personal data to non-EU/EEA countries and such protection can be adduced by requiring processors to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries ("**Standard Contractual Clauses**") pursuant to Commission Decision 2010/87/EU of 5 February 2010 as set out in Appendix 1;

WHEREAS, this DPA contains the terms and conditions applicable to the processing of such personal data by Processor as a commissioned data processor of Controller with the aim to ensure that the Parties comply with applicable data protection law.

In order to enable the Parties to carry out their relationship in a manner that is compliant with applicable law, the Parties have entered into the DPA as follows:

1 DEFINITIONS

1.1 For the purposes of this DPA, the terminology and definitions as used by the GDPR shall apply. In addition to that,

"**Data Exporter**"	shall mean the Controller, if (a) (i) the Controller is located in the EU/EEA or (ii) is located outside of the EU/EEA and is subject to the GDPR, and (b) transfers personal data to a Data Importer.
"**Data Importer**"	shall mean the Processor or Subprocessor that is located in a Third Country.
"**Member State**"	shall mean a country belonging to the European Union or to the European Economic Area.
"**Subprocessor**"	shall mean any further processor that is engaged by Processor as a sub-contractor for the performance of the Services or parts of the Services to be provided by Processor to Controller provided that such Subprocessor has access to the personal data of Controller when carrying out the subcontracted Services.
"**Third Country**"	shall mean a country outside of the EU/EEA that is not a White-List Country.
"**White-List Country**"	shall mean a country which is found by a decision of the EU Commission to ensure an adequate level of data protection within the meaning of Article 25 (2) of the Data Protection Directive (95/46/EC) and from May 25, 2018 within the meaning of Article 45 (1) General Data Protection Regulation.

1.2 This DPA has four Appendices. Appendix 1 contains the main body of the Standard Contractual Clauses. Appendix 2 contains the details of the processing and Appendix 3 contains the technical and organizational measures. Appendix 4 contains the list of processors. Appendix 2, Appendix 3 and Appendix 4 shall always apply. Appendix 1 shall apply in addition to this DPA only, if
(a) the Controller is located in the EU/EEA or is located outside of the EU/EEA and is subject to the GDPR, and
(b) the Processor is located in a Third Country. If Appendix 1 applies, Appendix 1 will prevail over this DPA in case of contradictions.

2 DETAILS OF PROCESSING

2.1 The details of the processing operations provided by Processor to Controller as a commissioned data processor (e.g., the subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects) are specified in Appendix 2 to this DPA.

3 OBLIGATIONS OF CONTROLLER

3.1 Controller is obliged to ensure compliance with any applicable obligations under the GDPR and any other applicable data protection law that applies to Controller as well as to demonstrate such compliance as required by Art. 5 (2) GDPR. Controller remains the responsible data controller for the processing of the personal data.

3.2 Controller is obliged to confirm before processing is carried out that the technical and organizational measures of Processor, as set out in Appendix 3, are appropriate and sufficient to protect the rights of the data subject and acknowledges that the Processor provides sufficient guarantees in this respect.

3.3 If required under local laws, Controller shall provide to the Processor a copy of the privacy notice that the Controller has delivered to the data subjects.

4 INSTRUCTIONS

4.1 Controller instructs Processor to process the personal data only on behalf of Controller. Controller's instructions are provided in this DPA and the Agreement. Controller is obliged to ensure that any instruction given to the Processor is in compliance with applicable data protection law. Processor is

obliged to process the personal data only in accordance with the instructions given by the Controller unless otherwise required by European Union law, Member State law or other applicable data protection law (in the latter case clause 5.4 (b) applies).

4.2 Any further instructions that go beyond the instructions contained in this DPA or the Agreement must be within the subject matter of this DPA and the Agreement. If the implementation of such further instructions results in costs for Processor, Processor shall inform Controller about such costs with an explanation of the costs before implementing the instructions. Only after Controller's confirmation to bear such costs for the implementation of the instructions, Processor is required to implement such further instructions. Controller shall give further instructions generally in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by Controller in writing without delay.

4.3 Processor shall immediately inform Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection law and request the Controller to withdraw, amend or confirm the relevant instruction. Pending the decision of the Controller on the withdrawal, amendment or confirmation of the relevant instruction, Processor shall be entitled to suspend the implementation of the relevant instruction.

5 OBLIGATIONS OF PROCESSOR

5.1 The Processor and persons authorized by Processor to process the personal data on behalf of Controller, in particular Processor's employees as well as employees of any Subprocessors, shall have committed themselves to confidentiality or shall be under an appropriate statutory obligation of confidentiality. Processor may not process personal data for purposes different than those that derive from or are related to the performance of its obligations under this DPA, or for purposes different than those instructed by the Controller.

5.2 Processor is obliged to implement the technical and organizational measures as specified in Appendix 3 before processing the personal data on behalf of Controller. Processor may amend the technical and organizational measures from time to time provided that the amended technical and organizational measures are not less protective as those set out in Appendix 3.

5.3 Processor is obliged to make available to Controller information in order to demonstrate compliance with the obligations of Processor laid down in Art. 28 GDPR. The Parties agree that this information obligation is met by providing Controller with an audit report upon request ("**Audit Report**"). To the extent additional audit activities are legally required, Controller may request inspections conducted by Controller or another auditor mandated by Controller ("**On-Site Audit**"). Such On-Site Audit is subject to the following conditions:

(a) On-Site Audits are limited to processing facilities and personnel of Processor involved in the processing activities covered by this DPA; and

(b) On-Site Audits occur not more than once annually or as required by applicable data protection law or by a competent supervisory authority or immediately subsequent to a material personal data breach that affected the personal data processed by Processor under this DPA; and

(c) may be performed during regular business hours, solely insubstantially disrupting the Processor's business operations and in accordance with Processor's security policies, and after a reasonable prior notice; and

(d) Controller shall bear any costs arising out of or in connection with the On-Site Audit at Controller and Processor.

Controller is obliged to create an audit report summarizing the findings and observations of the On-Site Audit ("**On-Site Audit Report**"). On-Site Audit Reports as well as Audit-Reports are confidential information of Processor and shall not be disclosed to third parties unless required by applicable data protection law or subject to Processor's consent.

5.4 Processor is obliged to notify Controller without undue delay:

(a) about any legally binding request for disclosure of the personal data by a law enforcement authority, unless otherwise prohibited, such as by a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(b) if Processor or Subprocessor is required pursuant to European Union law, Member State law or other applicable data protection law to which Processor or Subprocessor is subject to process the personal data beyond the instructions of Controller, before carrying out such processing beyond the instruction, unless that European Union law, Member State law or other applicable data protection law prohibits such information on important grounds of public interest - the notification to Controller shall specify the legal requirement under such European Union law Member State law or other applicable data protection law; and/or

(c) after Processor has documented reason to believe that a personal data breach at Processor or its Subprocessors has occurred that may affect the personal data of Controller covered by this DPA. In this case, Processor will assist Controller with Controller's obligation under applicable data protection law to inform the data subjects and the supervisory authorities, as applicable, by providing information according to Art. 33 (3) GDPR or other applicable data protection law as available to Processor. Processor shall implement remediation measures and corrective measures in order to prevent further breaches to occur again.

5.5 Processor is obliged to assist Controller with its obligation to carry out a data protection impact assessment as may be required by Art. 35 GDPR or under any other applicable data protection law and prior consultation as may be required by Art. 36 GDPR that relates to the Services provided by Processor to Controller under this DPA by means of providing the necessary and available information to Controller. Processor shall be obliged to provide such assistance only insofar that Controller's obligation can not be met by Controller through other means.

5.6 Processor is obliged - at the choice of the Controller - to delete or return to Controller all the personal data (and data storage media, which had been handed over by Controller, if any) which are processed by Processor on behalf of Controller under this DPA after the end of the provision of Services, and delete any existing copies unless European Union, Member State law or other applicable local law requires Processor to retain such personal data.

6 DATA SUBJECT RIGHTS

6.1 Controller is primarily responsible for handling and responding to requests made by data subjects.

6.2 Processor is obliged to assist Controller with appropriate and possible technical and organizational measures to respond to requests for exercising the data subjects' rights which are laid down in Chapter III of the GDPR or other applicable data protection laws.

7 SUBPROCESSING

7.1 Controller authorizes the use of Subprocessors engaged by Processor for the provision of the Services under this DPA. The same applies to the use of further Subprocessors engaged by Subprocessors, in which case the below applies accordingly. Processor shall choose such Subprocessor diligently. Processor remains responsible for any acts or omissions of its Subprocessors in the same manner as for its own acts and omissions hereunder. Controller approves the following Subprocessors:

Name	Address	Purpose of use
Software AG	Uhlandstraße 12 64297 Darmstadt Germany	provision of Cloud Services

7.2 Processor shall pass in writing (electronic form is sufficient) to Subprocessors the obligations of Processor under this DPA to the extent applicable to the subcontracted Services.

7.3 Processor may remove, replace or appoint suitable and reliable further Subprocessors at its own discretion in accordance with this clause:

(a) Processor shall notify Controller in advance of any changes to the list of Subprocessors as set out under clause 7.1. If Controller does not object in accordance with this clause 7.3 (b) within thirty days after receipt of Processor's notice the further Subprocessor(s) shall be deemed accepted.

(b) If Controller has a legitimate reason to object to a Subprocessor, Controller shall notify Processor thereof in writing within thirty days after receipt of Processor's notice. If Controller objects to the use of the Subprocessor, Processor shall have the right to cure the objection within thirty days after

Processor's receipt of Controller's objection If the objection has not been cured within thirty days after Processor's receipt of Controller's objection, either party may terminate the affected Service with reasonable prior written notice.

8 LIMITATION OF LIABILITY

8.1 Any liability arising out of or in connection with a violation of the obligations of this DPA or under applicable data protection law, shall follow, and be governed by, the liability provisions set forth in, or otherwise applicable to, the Agreement, unless otherwise provided within this DPA.

9 INDEMNITY

9.1 The Controller shall defend, indemnify, and hold harmless Processor and the officers, directors, employees, successors, and agents of Processor (collectively, “indemnified parties”) from all claims, damages, liabilities, assessments, losses, costs, administrative fines and other expenses (including, without limitation, reasonable attorneys' fees and legal expenses) arising out of or resulting from any claim, allegation, demand, suit, action, order or any other proceeding by a third party (including supervisory authorities) that arises out of or relates to the violation of Controller's obligations under this DPA and/or applicable data protection law.

10 DURATION AND TERMINATION

10.1 The term of this DPA is identical with the term of the Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Agreement.

11 GENERAL

11.1 In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this DPA shall prevail.

11.2 If any provision of this DPA is held to be invalid, illegal or unenforceable, the remaining provisions shall not be affected or impaired.

11.3 This DPA shall be governed by the same law as the Agreement.

APPENDIX 1

STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

1 Definitions

For the purposes of the Clauses:

(a) "personal data", "special categories of data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) "the data exporter" means the controller who transfers the personal data;

(c) "the data importer" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) "the sub-processor" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) "the applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) "technical and organisational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2 Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 2 which forms an integral part of the Clauses.

3 Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4 Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 3 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 3, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5 Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and

obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
(c) that it has implemented the technical and organisational security measures specified in Appendix 3 before processing the personal data transferred;
(d) that it will promptly notify the data exporter about:
(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
(ii) any accidental or unauthorised access, and
(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 3 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6 Liability
1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7 Mediation and jurisdiction
1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
(b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8 Cooperation with supervisory authorities
1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

9 Governing Law
The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10 Variation of the contract
The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11 Subprocessing
1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12 Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 2

DETAILS OF PROCESSING

Controller/Data Exporter
The Controller/Data Exporter performs the following activities relevant to the transfer (Controller to specify):

- The Controller/Data Exporter is providing business data necessary in course of use of and to assist in the analysis and resolution of Support Incidents reported in the Cloud Services of Processor/Data Importer

Processor/Data Importer
The Processor/Data Importer is a member of the Software AG group.

Data subjects
The personal data transferred concern the following categories of data subjects (Controller to specify):

- employees of Controller/Data Exporter
- potentially end customers of the Controller/Data Exporter

Categories of data
The personal data transferred concern the following categories of data (Controller to specify):

- Name
- Corporate Personnel ID
- Business e-mail address
- Telephone number
- IP Address

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (Controller to specify):

- The transfer of special categories of personal data is not anticipated.
- The Controller/Data Exporter decides which data is transmitted for the purpose of providing Cloud Services

Processing operations
The personal data transferred will be subject to the following basic processing activities:

- Processor/Data Importer processes Controller/Data Exporter Data with a Software as a Service /Platform as a Service in a public cloud infrastructure as defined in the Cloud Services agreement

Subject matter of the processing
The subject matter of the data processing under this addendum are the Controller/Data Exporter data processed in the cloud services as defined in the Cloud Services Attachment including the operation of a Cloud Service platform. To access the operated platform users need to be authenticated and authorized. User details will be used to create unique user id's that are used for authentication and authorization. Email addresses might be used to send notifications to the users as result of using services of the Cloud Service platform and corresponding support systems (e.g. Ticket system).

Nature and purpose of the processing
Processor/Data Importer processes the personal data of the data subjects on behalf of Controller/Data Exporter in connection with the following:

- The purpose of the data processing under this addendum the provisioning of the Cloud Services initiated by the Controller/Data Exporter. The Cloud Services processing systems and respective processing properties are defined in the Cloud Services Attachment

Signatures: See DPA signature page

APPENDIX 3

TECHNICAL AND ORGANIZATIONAL MEASURES

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor/Data Importer shall implement the following technical and organizational measures which have been confirmed as appropriate by the Controller/Data Exporter to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons. In assessing the appropriate level of security Controller/Data Exporter took account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

A. GENERAL TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

As of the Data Processing Agreement Effective Date Processor/Data Importer's entity set out in the relevant Cloud Services Attachment as the entity delivering the Cloud Services (hereinafter "**Cloud Service Unit**" or "**CSU**") is verified under ISO/IEC 27001 and agrees to maintain an information security program for the services that complies with the ISO/IEC 27001 standards or such other alternative standards as are substantially equivalent to ISO/IEC 27001 for the establishment, implementation, control and improvement of the Cloud Service Unit Security Standards.

1 CONFIDENTIALITY (ART 32 PARA. 1 LIT B GDPR)

1.1 **Access Control of Processing Areas**: Processor/Data Importer shall implement suitable measures to prevent unauthorized persons from gaining access to the data processing equipment where the personal data is processed. This is accomplished through the following measures:
- (a) Processor/Data Importer facilities access is strictly controlled. Physical access to sensitive IT facilities is regulated via Processor/Data Importer's Physical Access Policy.
- (b) Cloud Service Unit (CSU)'s Infrastructure as a Service sub-processor (IaaS Supplier), identified in the Cloud Services Attachment, maintains physical access control over the Cloud Services data processing equipment. The respective physical security mechanisms of the IaaS Supplier are reviewed by independent external audits in regards to ISO/IEC 27001 compliance.

1.2 **Access Control to Data Processing Systems**: Processor/Data Importer shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished through the following measures:
- (a) The following will be applied, among other controls, depending upon the particular Cloud Services subscribed: authentication via passwords and/or multi-factor authentication, documented authorization processes, documented change management processes and logging of access on several levels.
- (b) Access to Controller/Data Exporter data and systems is controlled in accordance with CSU's Access Control Policy aligned with the ISO/IEC 27001 Standard (Refer to Annex A 9 for additional details).

1.3 **Access Control to Use Specific Areas of Data Processing Systems**: Processor/Data Importer shall commit that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied, modified, or removed without authorization. This is accomplished through the following measures:
- (a) Operational System Administrative access is granted based on the principle of least privilege. Access controls to be applied include a documented change management process and the use of multi-factor authentication and encryption. This access is controlled in alignment with CSU's Access Control Policy, Clear Desk and Clear Screen Policy, Cryptographic Controls Policy and Data Privacy Policy.
- (b) Data transfer requirements of the CSU's Communication Security Policy are aligned with the ISO/IEC 27001 Standard (Refer to Annex A 13 for additional details).
- (c) Backup up of Controller/Data Exporter tenant data and protection of log files are controlled in alignment with the ISO/IEC 27001 Standard (Refer to Annex A 12 for additional details).

1.4 **Separation of Processing for Different Purposes**: Processor/Data Importer shall implement suitable measures to make sure that data collected for different purposes can be processed separately. This is accomplished through the following measures:
- (a) Processing of tenant content is directly encapsulated in the cloud application accessed via the cloud service. Access control to the tenant application is in the responsibility of the Controller/Data Exporter. All Controller/Data Exporter tenant content is directly encapsulated in the logically segregated tenant database.

1.5 **Pseudonymization**: In order to achieve the purposes of the commissioned data processing it is not possible to pseudonymize the Personal Data.

1.6 **Encryption**: Encryption of Controller/Data Exporter data at rest and in transit is ensured and controlled by the CSU's Cryptographic Controls Policy aligned with the ISO/IEC 27001 Standard (Refer to Annex A 10 for additional details).

2 INTEGRITY (ART 32 PARA. 1 LIT B GDPR)

2.1 **Input control**: Processor/Data Importer shall implement suitable measures to make sure that it can check and establish whether and by whom personal data has been inputted into data processing systems or removed. This is accomplished through the following measures:
- (a) The source of Personal Data is under the control of the Controller/Data Exporter, and Personal Data input into the system, is managed by secured file transfer (i.e., via web services or entered into the application) from the Controller/Data Exporter. Note - specific Cloud Services may permit Controllers/Data Exporters to use unencrypted file transfer protocols, in such cases, Controller/Data Exporter is solely responsible for its decision to use such unencrypted file transfer protocols.
- (b) Only authorized personnel will be able to access the production cloud infrastructure of Controller/Data Exporter data processing for the sole purpose of management and maintenance functions. All personnel have a unique user-id and use strong passwords according to CSU's Login and Password Policy and all such activities are monitored and logged.

2.2 **Transmission Control**: Processor/Data Importer implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished through the following measures:
- (a) For all production cloud environments IaaS provider security mechanisms are used to provide private, isolated areas for Processor/Data Importer Cloud where respective Cloud resources are launched in a defined virtual network. All scoped data is stored in a virtual cloud environment and is transmitted through HTTPS with up-to-date encryption ciphers.
- (b) Controller/Data Exporter tenant Data-at-rest for Cloud Services are encrypted. Except as otherwise specified for the Cloud Services (including within the ordering document or the applicable service specifications), transfers of data outside the Cloud Service environment are encrypted. The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted. Controller/Data Exporter is solely responsible for the results of its decision to use unencrypted communications or transmissions.
- (c) Data transfer requirements of the CSU's Communication Security Policy protect the transfer of Controller/Data Exporter tenant data through the use of all types of communication facilities.

3 AVAILABILITY AND RESILIENCE (ART 32 PARA. 1 LIT B GDPR)

3.1 **Availability Control**: Processor/Data Importer shall implement suitable measures to make sure that personal data is protected from accidental destruction or loss. This is accomplished through the following measures:
(a) Any changes to the production environments are fully monitored. CSU performs regular tenant backups to be able to restore virtual machine images and tenant data according to the Recovery Point Objectives and Recovery Time Objectives specified in the relevant Cloud Services Attachment.
(b) Control of availability for Cloud Services is ensured under CSU's Information Security Continuity Management and Operations Backup and Restore Controls aligned with the ISO/IEC 27001 Standard (Refer to Annex A 12 and 17 for additional details).
(c) The CSU's IaaS Supplier services are protected from utility service outages in alignment with the ISO/IEC 27001 standard as validated and certified by an independent auditor, and the identification of the person who carried them out is recorded.

3.2 **Resilience**: External access to all cloud production networks and systems is protected by Firewalls and Intrusion Detection Prevention Systems used to limit/filter network traffic. Cloud Services Disaster recovery is tested and reviewed on a yearly basis.

4 PROCESS FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANIZATIONAL MEASURES FOR ENSURING THE SECURITY OF THE DATA PROCESSING (ART. 32 PARA. 1 LIT. D GDPR)

4.1 **Data protection management**: In addition to the access control rules set forth in Sections Access control of processing areas and Access control to data processing systems, Controller/Data Exporter controls access to its Cloud Services and to Personal Data and other data through its authorized personnel. Personal Data from different Controllers/Data Exporters' environments are logically segregated. CSU's policy does not allow the replication of Controller/Data Exporter's production data to non-production environments unless explicitly requested by Controller/Data Exporter.

4.2 **Incident Response Management**: CSU has implemented a Security Incident Response Process and Security Incident Response Policy aligned with the ISO/IEC 27001 Standard (Refer to Annex A 16 for additional details). Controllers/Data Exporters are made aware of their responsibilities in the context of Cloud Service and Cloud Support Agreements. Security Incidents are tracked with the Processor/Data Importer incident management tool. Controller/Data Exporter point of contacts are notified via e-mail according to the Security Incident Response Policy. The incident response program of the IaaS Supplier (detection, investigation and response to incidents) has been developed in alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored.

4.3 **Data Protection by default (Art. 25 para. 2 GDPR)**: CSU has data protection policies and controls in place which prohibit CSU staff from accessing tenant data unless explicitly authorized and granted by the Controller/Data Exporter tenant administrator. All Controller/Data Exporter tenant content is directly encapsulated in the logically segregated tenant database. Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced. Default configurations of Cloud Services are designed to process only Personal Data required to deliver the service.

4.4 **Job Control**: Processor/Data Importer implements suitable measures to ensure that the personal data is processed in accordance with the instructions of the Controller. This is accomplished through the following measures:
(a) The control of Personal Data remains with Controller/Data Exporter, and as between Controller/Data Exporter and CSU, Controller/Data Exporter will at all times remain the Controller for the purposes of the Cloud Services, the Cloud Services Agreement, and the Data Processing Agreement. Controller/Data Exporter is responsible for compliance with its obligations as Controller under data protection laws, in particular for justification of any transmission of Personal Data to CSU (including providing any required notices and obtaining any required consents), and for its decisions and actions concerning the Processing and use of the data.
(b) CSU will process Personal Data solely for the provision of the Cloud Services, and will not otherwise (i) process or use Personal Data for purposes other than those set forth in the Cloud Services Agreement or as instructed by Controller/Data Exporter, or (ii) disclose such Personal Data to third parties other than CSU Cloud Operations supporting units or Subprocessors for the aforementioned purposes or as required by law.
(c) Access to Controller/Data Exporter data and systems are controlled in accordance with CSU's Access Control Policy and Operations Security Controls aligned with the ISO 27001 Standard (Refer to Annex A 9 and 12 for additional details).

4.5 **Job Control – Owners and Engineers**: Processor/Data Importer shall further implement suitable measures to monitor its cloud service system system administrators and to ensure that they act in accordance with instructions received. This is accomplished through the following measures:
(a) Individual appointment of system administrators;
(b) Adoption of suitable measures to log system administrators' access and keep those logs secure, accurate and unmodified for at least six months;
(c) Yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by importer and applicable laws; and
(d) Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned.

B. ADDITIONAL COUNTRY SPECIFIC MEASURES

No additional country specific measures applied.

APPENDIX 4

LIST OF PROCESSORS

The following organizations are located in third countries and for these the EU Standard Contractual Clauses listed in Appendix 1 will be concluded directly with the Customer, which means they take the role of being Processors. The Supplier has been given a power of attorney by the listed organizations to conclude the EU Standard Contractual Clauses with the Customer on their behalf.

#	Country	Name	Address	Data Processing Operation
1	Australia	Software AG Cloud APJ PTY Ltd.	Level 16, 201 Miller Street North Sydney, NSW 2060	Cloud Services and Support
2	Brazil	Software AG Brasil Informatica e Serviços Ltda	Av. das Nações Unidas 12.901, 33° andar, Torre Norte CEP 04578-000 São Paulo/SP	Cloud Services and Support
3	India	Software AG Chennai Development Center India Pvt Ltd	VBC Solitaire, 4th Floor, No. 47 & 49, Bazulla Road, T. Nagar 600 017 Chennai	Cloud Services and Support
4	India	Software AG Bangalore Technologies Private Ltd.	Embassy Tech Village 5th and 6th Floor, 2A East Tower, Marathahalli Outer Ring Road 560 103 Devarabisanahalli Bangalore	Cloud Services and Support
5	Malaysia	Software AG Operations Malaysia Sdn Bhd.	Suite 2B-22-1, Level 22, Block 2B, Plaza Sentral, Jalan Stesen Sentral 5, Kuala Lumpur Sentral, 50470 Kuala Lumpur	Cloud Services and Support
6	USA	Software AG Cloud Americas, Inc.	1209 Orange Street Wilmington, DE 19801	Cloud Services and Support
7	USA	Software AG USA, Inc.	11700 Plaza America Drive, Suite 700 Reston, VA 20190	Cloud Services and Support