

## OEM LICENSE AGREEMENT FOR CLOUD SERVICES

### General Terms And Conditions

The parties agree that their contractual relationship shall be governed by the general terms and conditions set forth below as well as all applicable exhibits, schedules, amendments or addendum attached hereto or to any Order Form or referenced herein as part of the agreed terms, all of which are made an integral part hereof (collectively referred to herein as the "Agreement.").

### 1. DEFINITIONS

As used in this Agreement, the following terms shall have the following meanings:

"Affiliate" of a party means any legal entity in which a party, directly or indirectly, holds more than fifty percent (50%) of the shares or voting rights or controls or is under common control with that legal entity. "Control" means the direct or indirect possession of the power to direct or cause the direction of the management and policies of an entity, whether through ownership, by contract or otherwise. Any such company shall be considered an Affiliate for only such time as such interest or control is maintained.

"Bundled Service" means the combined offering of SAP's Cloud Services that are used in conjunction with the OEM Services.

"Cloud Service" means SAP's hosted, on-demand Cloud Services listed in Exhibit A hosted and made available by SAP and ordered by OEM pursuant to a Cloud Service Schedule (for End User Subscription) and resold for use in conjunction with OEM Services to End Users.

"Cloud Service Schedule" means a service schedule that references this Agreement and mutually executed by SAP and OEM for the Cloud Service ordered by OEM on behalf of each End User, including information on Cloud Services, Platinum Support Fee (if application), and such other information necessary for SAP's provision of such services and such other terms and conditions as mutually agreed upon by the parties in writing.

"Confidential Information" means, with respect to SAP, (a) the Cloud Services and all information which SAP protects against unrestricted disclosure to others, including but not limited to all (i) computer software (both object and source codes) and related Service documentation or specifications; (ii) techniques, concepts, methods, processes and designs embodied in or relating to the Service; and (iii) all application program interfaces, system infrastructure, system security and system architecture design relating to the Service; and (b) SAP research and development, product offerings, pricing and availability, technical drawings, algorithms, processes, ideas, techniques, formulas, data, schematics, trade secrets, know-how, improvements, marketing plans, forecasts and strategies. In addition to the foregoing, Confidential Information of either SAP or Partner (the party disclosing such information being the "Disclosing Party") may also include information which the Disclosing Party protects against unrestricted disclosure to others that (i) the Disclosing Party or its representatives designates as confidential at the time of disclosure; or (ii) should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding its disclosure; including, without limitation, information about or concerning any third party that is disclosed to Receiving Party under this Agreement.

"CPPD Schedule" means SAP's then-current SAP OEM Cloud Service Schedule for Commissioned Processing of Personal Data, whether made available to OEM in writing or online at an SAP website to be identified by SAP. A current copy of the CPPD Schedule as of the date of this Agreement is attached hereto as Annex 1.

"Documentation" means SAP's then-current technical and functional documentation for the Cloud Service which is delivered or made available with the Cloud Service.

"End User" means OEM's customer licensing or using the OEM Services from OEM.

"End User Agreement" means a written agreement entered into between OEM and any End User pursuant to which the End User purchases subscriptions to the Bundled Services.

"End User Data" means any content, materials, data and information that End Users or its Named Users enter into the Cloud Service.

"Group Company" means any person, partnership, joint venture, corporation, company or other form of enterprise, domestic or foreign, located in the Territory, who (i) is under the Control of SAP or (ii) has Control over SAP.

"Integration" means applications, scripts, commands or instructions that use the API to connect to the Cloud Services.

"Intellectual Property Rights" means patents of any type, design rights, utility models or other similar invention rights, copyrights, mask work rights, trade secret or confidentiality rights, trademarks, trade names and service marks and any other intangible property rights, including applications and registrations for any of the foregoing, in any country, arising under statutory or common law or by contract and whether or not perfected, now existing or hereafter filed, issued, or acquired.

"Named User" means End User's and its Affiliates' employees, agents, contractors, consultants, suppliers or other individuals who are authorized by End User to use the Cloud Service.

"OEM Service" shall mean OEM's online services specified in Exhibit B that (i) add significant and primary functionality to the scope of Cloud Services, and (ii) are provided to End Users located in the Territory by OEM through remote access via the

Internet, and may include the provision of the administration, redundancy, back-up and technical support services as they apply to the deployment and management of the Bundled Services.

“Order Form” means any order form that references this Agreement and mutually executed by SAP and OEM, including information regarding specified Cloud Services, OEM Services, territory, the term of the Agreement and subscription fees for each Cloud Service Schedule executed by OEM for the purchase of the Cloud Services on behalf of each End User during the term of the Agreement.

“SAP” means the SAP entity identified by this OEM License Agreement for Cloud Service or the Order Form that is a party to this Agreement.

“SAP Materials” means any software, programs, tools, systems, data, or other materials made available by SAP to OEM in the course of the performance under this Agreement including, but not limited to, the Cloud Service and Documentation, as well as any information, materials or feedback provided by OEM to SAP relating to the Cloud Service and Documentation.

“Territory” means the territory specified in Exhibit A, and subject to Section 10 of this Agreement (Import and Export Control).

“Trademarks” means the trademarks, service marks, trade names, service names, proprietary words, symbols and other logos of SAP or any of its Group Companies.

Other defined terms shall have the meanings set forth herein. References to “Exhibits” shall include all sub-exhibits of such Exhibit (i.e. references to Exhibit A will include Exhibits A-1, A-2 and A-3 etc) and such Exhibits may be attached to this Agreement or any Order Form.

“Work Product” means any work product or tangible results produced by or with SAP pursuant to this Agreement, including in the course of providing support, training or configuration services to OEM or its End Users. Work Product includes works created for or in cooperation with OEM or its End Users, but does not include any End User Data, OEM Confidential Information or the Cloud Service. For clarity, some services may be performed under a statement of work, which statement of work will be governed by the terms and conditions of this Agreement.

## **2. GRANT OF RIGHTS**

### **2.1 Grant of License.**

- (a) Integration, Demonstration and Support Use Rights. Subject to the terms of this Agreement, SAP grants OEM during the term of this Agreement a nonexclusive, nontransferable, non-perpetual right to use in the Territory the Cloud Services solely to the extent necessary to (i) develop an Integration between the Cloud Service and OEM Services, and (ii) use and access the Cloud Services to demonstrate for potential End Users and support the Cloud Service as part of providing the Bundled Services to End Users. OEM shall be responsible for any additional software, migration tools, or third party products needed to integrate and use the Cloud Services.
- (b) Cloud Services Subscription License. Subject to the terms of this Agreement, SAP grants OEM during the term of the Agreement a non-exclusive, limited, non-transferable, non-perpetual right in the Territory to market and resell subscriptions to the Cloud Services only for use in conjunction with OEM Services to End Users. SAP shall provide the Cloud Service to End Users in accordance with the Cloud GTC (as defined in Section 2.1(c)), the applicable Order Form and Cloud Service Schedule. Notwithstanding anything to the contrary provided in the Cloud GTC, OEM and its End Users shall have access only to the most current version of the Cloud Service made generally available by SAP to its customers, and SAP may change or modify the Cloud Service at any time
- (c) In utilizing the Cloud Services in accordance with this Agreement, OEM agrees to be bound by the General Terms and Conditions for Cloud Services and all documents referenced thereby, including without limitation any product-specific Supplemental Terms and Conditions available at <http://www.sap.com/agreements/north-america> (please select “Software License Agreements” => “SAP Cloud Agreements” => “United States”) current as of the effective date of the applicable Order Form (collectively, the “Cloud GTC”), except to the extent inconsistent with this Agreement.

2.2 Bundled Services. OEM may market and resell the Cloud Services only for use in conjunction with OEM Services in accordance with the terms of this Agreement and Order Form. The End User Agreement shall permit the End User’s use of the Cloud Service only with the Bundled Service, with data access limited to data created or used by the OEM Service (referred to as a “Restricted License”). OEM may resell the Cloud Services only directly to its End Users. OEM is not permitted to appoint any resellers, distributors or other third parties to resell the Cloud Services to its End Users. OEM shall impose on the End Users the restrictions as set forth in this Section 2.2. OEM shall promptly notify SAP of any violations of this Section 2.2 by any End Users or other third parties.

2.3 Third Party Service. OEM may resell the Cloud Service, which may include the use of third party technology or services from third party suppliers, in accordance with the Agreement only to the extent SAP continues to have rights to resell the technology or service of such third-party supplier.

## **3. GENERAL OBLIGATIONS OF AND LIMITATIONS TO OEM**

3.1 OEM shall contract with its End Users directly for the Bundled Services. OEM shall secure the End User’s consent to an End User Agreement with terms that are not materially less protective of SAP than SAP’s Cloud GTC (as defined in Section 2.1(c)) current as of the commencement date of each subscription term of the Cloud Service (“Minimum Terms”), and SAP shall be named as a third party beneficiary under such End User Agreement. The Minimum Terms shall also require that the Cloud Service may only be used as part of the Bundled Service, and notwithstanding anything to the contrary provided in the Cloud GTC, the End Users shall have access only to the most current version of the Cloud Service made generally available by SAP to its customers, and SAP may change or modify the Cloud Service at any time. Where OEM decides to use the Cloud GTC for its own purposes, OEM shall replace the references to SAP in the Cloud GTC with OEM and SAP shall be made a third party beneficiary under the End User Agreement. OEM shall also ensure

that each of its End Users utilizes the Cloud Services only in conjunction with the Bundled Service. OEM shall be liable to SAP for any breach of the terms of such End User Agreement to the same extent as OEM would be liable to SAP under this Agreement for such a breach by OEM.

- 3.2 OEM shall reasonably cooperate with SAP to enforce the limitations and requirements imposed according to Sections 2.2 and 3.1 to the fullest extent possible.
- 3.3 End Users shall contract with OEM directly for the Bundled Service. Pricing, billing and all other terms and conditions relating to End Users' use of the Cloud Service shall be solely between End Users and OEM. For clarity, pricing for the Cloud Service must be incorporated into the Bundled Services pricing and may not be itemized separately unless otherwise agreed to in writing by SAP in advance (such as for upsells into existing OEM customers).
- 3.4 OEM shall not make any representations or warranties regarding the functionality or performance of the Cloud Service other than in accordance with the Cloud GTC.
- 3.5 OEM shall be responsible for implementation and configuration of the Bundled Service for its End Users. OEM shall contract directly with End Users for such services and will be solely responsible for invoicing and collecting fees from End Users for such services. If OEM chooses to provide implementation and configuration services directly to its End Users: (i) OEM must first complete SAP's implementation certification program (for which additional fees apply), and (ii) OEM must engage SAP's delivery assurance team (for which additional fees apply) in the event that OEM wishes to provide such services for the first six End Users. Alternatively, OEM may subcontract implementation and configuration services to SAP or SAP's certified implementation partners. For clarity, where OEM subcontracts such services, OEM will nonetheless project manage the implementation and configuration services for the End Users.

#### **4. ORDERS, PAYMENT AND TAXES**

- 4.1 OEM will independently establish prices and terms for the Bundled Services, provided such terms include those required by the Agreement.
- 4.2 Except as otherwise agreed upon by the parties, OEM agrees that it must purchase on behalf of each End User: (i) a three year subscription term to the Cloud Service (which term shall not be longer or shorter than three years), and (ii) Platinum Support (as available). OEM shall execute a Cloud Service Schedule with SAP for each End User subscription of the Cloud Service, and submit the Cloud Service Schedule to SAP together with the CPPD Schedule executed by the End User ordering the Cloud Service in accordance with Section 12 of this Agreement. The Cloud Service Schedule shall include such information as required by SAP for Cloud Service subscriptions, including without limitation (i) the Cloud Service subscription being ordered, (ii) customer name (no abbreviations), customer address (street, city, postal code, country), group (if any) and the total number of Named Users (or such other pricing unit) for each Cloud Service, (iii) the subscription term and (iv) all information necessary to enable SAP to set up access of the Cloud Services for each End User. SAP reserves the right to reject a Cloud Service Schedule and/or the CPPD Schedule in its sole and reasonable discretion, including due to such schedules in form or content is not in compliance with the terms of this Agreement.
- 4.4 OEM shall pay to SAP the fees for the Cloud Service due under this Agreement, including the applicable Order Form and Cloud Service Schedule, within thirty (30) days of the date of invoice. OEM can offset claims only if they are uncontested or awarded by final and binding court or arbitration court order. Except as expressly set forth in this Agreement, all payments made hereunder are non-refundable, and all amounts due hereunder are non-cancelable.
- 4.5 Subject to the increase in fees during the Renewal Term (as defined below) set forth below, the fees set forth in a Cloud Service Schedule will be fixed for the then-current committed subscription term. The term of the Cloud Service Schedule executed by OEM shall continue in effect as described in the Cloud Service Schedule. Following the subscription term of the applicable Cloud Service Schedule, the subscription shall automatically renew for additional one-year terms (each, as applicable, a "Renewal Term"). Fees for automatic Renewal Terms will be invoiced as set forth in the Cloud Service Schedule, except that SAP may apply an increase to such fees to account for changes in consumer prices generally or increases in fees of third party technology or service used in the applicable SAP Cloud Service over the preceding term of the applicable Cloud Service Schedule. Any pricing changes, which will be fixed for the entirety of such automatic Renewal Terms, will be reflected on the initial invoice for the Renewal Term. SAP or OEM may give the other party written notice (email acceptable) of non-renewal as follows: at least thirty (30) days prior to the end of the relevant subscription term for OEM's notice, and at least 90 days prior to the end of the relevant subscription term for SAP's notice.
- 4.6 OEM may add additional Named Users or other fee-based metrics for any End User during the term of the Cloud Service Schedule by executing an addendum or additional schedule to such Cloud Service Schedule with SAP, as applicable. The term of each addendum or schedule shall be co-terminus with the then-current term of the Cloud Service Schedule for such End User irrespective of the effective date of such addendum and all fees shall be prorated accordingly. Upon renewal of the Cloud Service Schedule, the term for all Named Users or other fee-based metric added to the Cloud Service Schedule prior to renewal shall be the same as specified in the Cloud Service Schedule, unless the parties agree to extend the term in the addendum. Termination of the initial Cloud Service Schedule shall also encompass termination of Cloud Service Schedule for additional Named Users. A Cloud Service Schedule for additional Named Users shall be deemed an amendment to the initial Cloud Service Schedule.
- 4.7 OEM shall ensure that each End User is contractually obligated to monitor each End User's use of the Cloud Service. OEM shall require End User to report to OEM any actual use in excess of the number of Named Users or the amount of any fee-based metric. OEM shall forward such information to SAP without undue delay. Based on such information, SAP will calculate the amount of fees payable under the respective Cloud Service Schedule. OEM agrees to execute an addendum and pay all requisite fees in accordance with the terms of this Agreement from the date the excess use began. For the avoidance of doubt, OEM shall not be entitled to claim any reduction of the fees payable under each Cloud Service Schedule or Order Form.

- 4.8 Except as expressly set forth in this Agreement, the Order Form or Cloud Service Schedule, all purchases of subscriptions hereunder are non-cancelable after submission of the Cloud Service Schedule to SAP and all fees are non-refundable. Unless otherwise specified herein, OEM may not reduce the Named Users or other fee-based metrics during the term of the Cloud Service Schedule regardless of any termination, nonpayment, nonuse or other conduct or inaction on the part of the corresponding End User. This shall also apply in case SAP suspends access to the Cloud Service for a particular End User for breach of the Minimum Terms. OEM shall have no right to withhold or reduce fees under this Agreement or set off any amount against fees owed for alleged defects in the Cloud Service.
- 4.9 All fees not paid when due shall accrue interest at the lesser of 1.5% per month or the maximum rate allowed under applicable law, and may result in suspension of OEM and its End Users' ability to access the Cloud Service until payment is made.
- 4.10 Taxes.
- (a) Fees and other charges described in this Agreement, Order Forms or Cloud Service Schedule do not include federal, state or local sales, VAT, GST, foreign withholding (including foreign income withholding), use, property, excise, service, or similar taxes ("Tax(es)") now or hereafter levied, all of which shall be for OEM's account. Any applicable direct pay permits or valid tax-exempt certificates must be provided to SAP prior to the execution of this Agreement. If SAP is required to pay Taxes, OEM shall reimburse SAP for such amounts. OEM hereby agrees to indemnify SAP for any Taxes and related costs, interest and penalties paid or payable by SAP.

## 5. AUDITS

- 5.1 Audits. During the term of this Agreement and for three (3) years thereafter, OEM will maintain relevant records regarding its use and subscription of the Cloud Service for each of its End Users. Upon reasonable notice to OEM, SAP may audit, at SAP's expense, the records of OEM and any other person acting on its behalf relating to OEM's activities under this Agreement to determine OEM's compliance hereunder, including the compliance with the Minimum License Terms and the calculation of the fees due under this Agreement, applicable Order Forms and Cloud Service Schedule. In the event any such audit reveals that OEM has underpaid SAP, then, in addition to immediately settling the outstanding amount and such other remedies as SAP may have, OEM shall pay or reimburse to SAP the cost of the audit.

## 6. SUPPORT

- 6.1 End User Support by OEM. OEM shall provide Tier 1 and Tier 2 support to End Users for the Cloud Service. For purposes of this Agreement, Tier 1 support includes responding to calls and inquiries from End Users or its Named Users. Tier 2 support includes: (i) verification that an inquiry is received from a valid End User; (ii) acknowledgment to the End User of receipt of such inquiry; (iii) checking lists of known issues and solutions/workarounds; (iv) leveraging OEM training, experience or other appropriate internal resources to find a resolution; and (v) if the reported issue is known or found, providing the resolution to the End User and assisting with its implementation. In the event OEM is unable to resolve the issue after exhausting its own internal resources, OEM may escalate the issue to SAP for Tier 3 support. Escalation to SAP for Tier 3 support shall include: (a) isolation, identification and reproduction of the unresolved issue reported by an End User; (b) documentation and submission of the unresolved issue to SAP as directed by SAP; and (c) communication back to through OEM to End User regarding any updates and assistance in implementing any resolutions received from SAP. OEM will appoint at least two system administrators ("**System Administrators**") who may contact SAP directly for escalations. System Administrators must be trained and certified by SAP prior to designation by OEM. Training requirements and fees will be at OEM's expense and at SAP's then current published rates. In addition, OEM will designate: (i) one account manager per End User, and (ii) up to five (5) named contacts per End User, who may access the online support portal on behalf of the applicable End User. In general, OEM is expected to resolve the majority of the inquiries received by OEM from End Users directly, which may include, but are not limited to, "how to", feature questions, or "Service not working" issues. Without limiting SAP's right to terminate or other available remedies, upon OEM's failure to provide adequate support and upon SAP's request, the parties shall in good faith agree on an alternative solution for the provision of Tier 1 and Tier 2 support to the End User (including resolution of the cost and expenses for such alternative solution).
- 6.2 OEM Support. SAP shall provide Platinum Support (where available) for applicable Cloud Service to OEM as described in the Cloud GTC, provided that OEM purchases Platinum Support for such applicable Cloud Service for each End User. SAP shall be responsible for responding to issues escalated and submitted by OEM that contain the required information as directed by SAP. SAP will respond directly to OEM as outlined in SAP's then-current support policy for the applicable Cloud Service, which SAP may change in its sole discretion and make available to OEM in writing or online at an SAP website as SAP may designate. SAP shall have no obligation to support (i) the combination, operation or use of the Cloud Service with any third party service or otherwise contemplated in the Documentation, if the problem cannot be reproduced in the Cloud Service without such combination or use with such third party service; or (ii) problems due to causes external to the Cloud Service or otherwise beyond the reasonable control of SAP.

## 7. INTELLECTUAL PROPERTY AND CONFIDENTIALITY

- 7.1 Intellectual Property Rights. The Cloud Service, Documentation, SAP Materials, Trademarks, Integration, Work Product, and all Intellectual Property Rights embodied in the foregoing, shall be the sole and exclusive property of SAP or its Group Companies, or its or their licensors. All rights in and to the Cloud Service, Documentation, Integration, Work Product, SAP Materials and Trademarks not expressly granted in this Agreement are reserved by SAP.
- 7.2 Trademarks; Logos
- (a) Except as otherwise provided in Section 7.2(b) below, nothing in this Agreement grants OEM the right to use or display any SAP or Group Company's Trademarks. OEM shall not remove, delete or in any manner alter the Trademarks or other Intellectual Property Rights notices of SAP, Group Companies and SAP's suppliers, if any, appearing on the Cloud Services, Documentation, Work Product, sales, marketing or training materials or any other

materials as delivered to OEM by SAP. SAP shall have the sole and exclusive right to protect and defend the Trademarks, at its sole cost and expense. OEM shall reasonably cooperate with SAP, at SAP's expense, in the defense and protection of the Trademarks, and shall promptly advise SAP of the use of any mark infringing any of the SAP Trademarks of which it has knowledge.

- (b) SAP grants to OEM during the term of the Agreement a revocable, nonexclusive, nontransferable license to use the appropriate SAP partner logo provided by SAP to OEM in the then-current SAP Branding Guide in the Territory in accordance with the terms of this Section 7.2 solely as necessary to market the Bundled Service to potential customers in the Territory as set forth in this Agreement. This license to use the SAP partner logo includes the right to use the SAP corporate logo as part of the SAP partner logo (hereinafter "SAP Logo Trademarks"). OEM is not permitted to grant sublicenses to SAP Logo Trademarks. When using SAP Logo Trademarks, OEM must adhere to all requirements and obligations of the then-current SAP Branding Guide.
- (c) OEM shall not contest the validity of the SAP Trademarks or support the contesting of its validity and shall not derive any right against SAP through its permitted use of SAP Logo Trademarks. In its use of SAP Logo Trademarks, OEM shall indicate that the SAP Logo Trademarks are registered by and for SAP. In this context OEM acknowledges that SAP AG or its applicable Group Company, as the case may be, is the sole owner of rights in the SAP Trademarks. OEM undertakes to make all those declarations and provide all those documents for the benefit of SAP as SAP or SAP AG may require in the prosecution of its rights in the SAP Trademarks. All advertising and sales material used by OEM for the Cloud Service must bear the notices prescribed by SAP or its Group Companies concerning trademarks and other identifying marks. OEM shall not register SAP's and/or SAP AG's name (or any domain name or trademark) or SAP AG's logo (or any names, logos, domain names or trademarks which are confusingly similar to any of them) for itself or permit third parties to use or otherwise exploit SAP's and/or SAP AG's name, domain name, logo or trademark (or any name, logo, trademark or domain name which are confusingly similar to any of them). OEM must, at SAP's choice, either transfer any rights regarding such name, logos, trademarks and domain names to SAP as soon as they arise or permit SAP to exploit them.
- (d) OEM shall provide samples of its advertising copy and sales literature, in their original language and in English, as applicable, upon SAP's request. SAP reserves the right to review and approve all uses of SAP's Trademarks in OEM's advertising and promotion of the Cloud Service, prior to use. Such approval will not limit OEM's obligation to comply with all applicable laws and will not be deemed an endorsement or approval of any advertising content. OEM shall make no representations regarding the Cloud Service except as consistent with SAP's own promotional and technical materials or as SAP may otherwise provide or approve in writing.

7.3 SAP retains all right, title and interest in and to any Work Product, provided, however, that SAP hereby grants OEM a royalty-free, fully paid-up, nonexclusive, worldwide, transferable (only to a successor in interest by way of merger, reorganization or sale of all or substantially all assets or equity), sublicensable license during the term of the Agreement to use, copy, modify or distribute the Work Product solely to provide the Bundled Service to End Users in accordance with the terms of this Agreement.

7.4 Confidential Information.

- (a) Confidential Information shall not be used or reproduced in any form except as required to accomplish the intent of this Agreement. Any reproduction of any Confidential Information of the other party shall remain the property of the Disclosing Party and shall contain any and all confidential or proprietary notices or legends which appear on the original. With respect to the Confidential Information of the other, each party (a) shall take all Reasonable Steps (defined below) to keep all Confidential Information strictly confidential; and (b) shall not disclose any Confidential Information of the other to any person other than individuals whose access is necessary to enable it to exercise its rights and/or perform its obligations hereunder and who are under obligations of confidentiality substantially similar to those set forth herein. As used herein "Reasonable Steps" means those steps the receiving party takes to protect its own similar proprietary and confidential information, which shall not be less than a reasonable standard of care. Confidential Information of either party disclosed prior to execution of this Agreement shall be subject to the protections afforded hereunder.
- (b) The above restrictions on the use or disclosure of the Confidential Information shall not apply to any Confidential Information that: (a) is independently developed by the receiving party without reference to the Disclosing Party's Confidential Information, or is lawfully received free of restriction from a third party having the right to furnish such Confidential Information; (b) has become generally available to the public without breach of this Agreement by the receiving party; (c) at the time of disclosure, was known to the receiving party free of restriction; or (d) the Disclosing Party agrees in writing is free of such restrictions.
- (c) OEM shall not disclose the terms and conditions of this Agreement or the pricing contained herein to any third party. Neither party shall use the name of the other party in publicity, advertising, or similar activity, without the prior written consent of the other, except that OEM agrees that SAP may use OEM's name in customer or partner listings or, at times mutually agreeable to the parties, as part of SAP's marketing efforts (including without limitation reference calls and stories, press testimonials, site visits, SAPPHERE participation). SAP will make reasonable efforts to avoid having the reference activities unreasonably interfere with OEM's business.
- (d) OEM may provide, or SAP may solicit, input regarding the Cloud Service, including, without limitation, comments or suggestions regarding the possible creation, modification, correction, improvement or enhancement of the Cloud Service or any other SAP or SAP site, service or product, or input as to whether OEM believes SAP or its Group Companies' development direction is consistent with OEM or its End Users' business and IT needs, the technology marketplace in general, and the like (collectively "Feedback"). OEM acknowledges and agrees that any information disclosed by OEM during discussions related to Feedback shall be considered SAP Confidential Information and shall be protected from disclosure in accordance with the terms of this Agreement. In order for SAP to utilize such Feedback, OEM hereby grants to SAP and its Group Companies a non-exclusive, perpetual, irrevocable, worldwide,

royalty-free license, with the right to sublicense to SAP's licensees and customers, under OEM's relevant intellectual property rights, to use, publish, and disclose such Feedback in any manner SAP chooses and to display, perform, copy, make, have made, use, sell, and otherwise dispose of SAP's and its sublicensee's products or services embodying Feedback in any manner and via any media SAP chooses, without reference to the source. SAP shall be entitled to use Feedback for any purpose without restriction or remuneration of any kind with respect to OEM and/or OEM's representatives. OEM acknowledges that the information related to the Cloud Service disclosed by SAP under this Agreement is only intended as possible strategies, developments, and functionalities of the Cloud Service and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development.

- 7.5 OEM shall inform SAP as soon as practicable if it is aware of any third party that has unauthorized access to the Cloud Service (including End Users that exceed licensed levels) or markets, sells, or uses the Cloud Service or SAP Materials without authorization. Moreover, OEM must also assist SAP in every reasonable way in the pursuance of SAP's rights and, upon consultation with SAP, must immediately take all steps for the protection of those rights. OEM must temporarily stop selling and marketing the Cloud Service to any such third party unless and until such ambiguity is resolved to OEM's and SAP's satisfaction.
- 7.6 The parties recognize that either party has the right to develop independently software or services that would compete with the other party's software or services without use of any Confidential Information disclosed by such other party hereunder. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with Confidential Information disclosed hereunder. The term "residuals" means information in non-tangible form, which may be retained inadvertently in the unaided memory by persons who have had access to the Confidential Information, including ideas, concepts, know-how or techniques contained herein, so long as such persons have not studied the information for the purpose of replicating the same from memory. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay fees or royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

## **8. INDEMNIFICATION**

### **8.1 Third Party Rights.**

- (a) SAP shall defend OEM and its Affiliates against claims brought against OEM by any third party alleging that OEM or its End User's use of the Cloud Service, in accordance with the terms and conditions of this Agreement and the applicable Order Forms, constitutes a direct infringement or misappropriation of a patent claim(s), copyright or trade secret rights, and SAP will pay damages finally awarded against OEM (or the amount of any settlement SAP enters into) with respect to such claims. This obligation of SAP shall not apply if the alleged infringement or misappropriation results from use of the Cloud Service in conjunction with any other software or service (including OEM Service) if such claim could have been avoided without such use, or unlicensed activities or use of the Cloud Service in violation of this Agreement or to free (no fee) or trial licenses of the Cloud Service. This obligation of SAP also shall not apply if OEM fails to timely notify SAP in writing of any such claim, however OEM's failure to provide or delay in providing such notice shall not relieve SAP of its obligations under this Section except to the extent SAP is prejudiced by OEM's failure to provide or delay in providing such notice. SAP is permitted to fully control the defense and any settlement of any such claim as long as such settlement does not include a financial obligation on or admission of liability by OEM. In the event OEM declines SAP's proffered defense, or otherwise fails to cede full control of the defense to SAP's designated counsel, then OEM waives SAP's obligations under this Section 8.1. OEM shall reasonably cooperate in the defense of such claim and may appear, at its own expense, through counsel reasonably acceptable to SAP. SAP expressly reserves the right to cease such defense of any claim(s) in the event the Cloud Service is no longer alleged to infringe or misappropriate, or is held not to infringe or misappropriate, the third party's rights. SAP may settle any claim on a basis requiring SAP to substitute for the Cloud Service alternative substantially equivalent non-infringing services. OEM shall not undertake any action in response to any infringement or misappropriation, or alleged infringement or misappropriation of the Cloud Service that is prejudicial to SAP's rights.
- (b) In the event a claim under Section 8.1 is made or alleged or in SAP's reasonable opinion is likely to be made or be alleged, SAP may, at its sole option and expense: (i) procure for OEM and its End Users the right to continue using the Cloud Service under the terms of this Agreement; or (ii) replace or modify the Cloud Service to be non-infringing without material decrease in functionality. If the foregoing options are not reasonably available, SAP may terminate this Agreement and refund to OEM all prepaid fees for the remainder of its term after the date of termination.
- (c) THE PROVISIONS OF THIS SECTION 8.1 STATE THE SOLE, EXCLUSIVE, AND ENTIRE LIABILITY OF SAP AND ITS GROUP COMPANIES TO OEM, AND IS OEM'S SOLE REMEDY, WITH RESPECT TO ANY CLAIMS OF INFRINGEMENT OR MISAPPROPRIATION OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS. The liability limitations contained in Section 15 shall apply to all claims made under Section 8.1. Any limitations to the liability and obligations of SAP according to Sections 8.1 and 15 shall also apply for the benefit of Group Companies and their respective licensors.

- 8.2 Indemnification by OEM. OEM shall defend SAP and its Group Companies against claims brought against SAP or its Group Companies by any third party arising from or related to (i) any use of the Cloud Service in violation of any applicable law or regulation; or (ii) an allegation that the OEM or End User Data or OEM's or its End User's use of the Cloud Service in violation of this Agreement violates, infringes or misappropriates the rights of a third party, or (iii) OEM's representations not authorized by SAP, or (iv) OEM or its Affiliates' breach of this Agreement, including but not limited to, any breach or violation of applicable export laws or regulations, or action in excess of OEM's authority hereunder or OEM's failure to comply with the End User licensing requirements set forth in this Agreement, or (v) any agreement between OEM and its distributors, resellers or End Users, or (vi) a claim that OEM Service infringes, misappropriates or violates any patent, copyright or trademark of any third party or OEM's combining (or its authorizing others to combine) the Cloud Service with any products or service not provided by SAP, (vii) a third party's assertion that OEM acted as SAP's agent or otherwise on its behalf End User or (viii) any End User claim brought against SAP in connection with the End User

Agreement. OEM will pay damages finally awarded against SAP and its Group Companies (or the amount of any settlement OEM enters into) with respect to such claims. The foregoing shall apply regardless of whether such damage is caused by the conduct of OEM, its resellers, distributors, agents or its End Users and/or their respective Named Users or by the conduct of a third party using OEM or End Users' access credentials. This obligation of OEM shall not apply if SAP fails to timely notify OEM in writing of any such claim, however SAP's failure to provide or delay in providing such notice shall not relieve OEM of its obligations under this Section except to the extent OEM is prejudiced by SAP's failure to provide or delay in providing such notice. OEM is permitted to fully control the defense and any settlement of any such claim as long as such settlement does not include a financial obligation on or admission of liability by SAP or otherwise obligates SAP to specific performance. In the event SAP declines OEM's proffered defense, or otherwise fails to cede full control of the defense to OEM's designated counsel, then SAP waives OEM's obligations under this Section 8.2. SAP shall reasonably cooperate in the defense of such claim and may appear, at its own expense, through counsel reasonably acceptable to OEM.

## 9. TERM AND TERMINATION

- 9.1 This Agreement begins on the Effective Date of the first Order Form entered into between OEM and SAP and shall continue for an initial term of three years ("Initial Term"), unless earlier terminated as set forth herein. The Agreement may be extended by a term to be defined upon mutual written agreement of the parties only.
- 9.2 This Agreement, any Order Form and Cloud Service Schedule may be terminated by either party for good cause upon written notice to the other in accordance with the following:
- (a) thirty days after a party gives the other party notice of breach of any provision of the Agreement (other than OEM's breach of its obligations under Sections 2.1, 7.1-7.6, 10, 11, 12 or 13.1, which breach shall give right to immediate termination), Order Form or Cloud Service Schedule, unless the breaching party has cured such breach during such thirty day period;
  - (b) immediately if OEM does not pay on the due date any amount payable to SAP unless payment is made within 30 days of its due date;
  - (c) immediately if a party (1) commences negotiations with one or more of its creditors with a view to rescheduling major parts of its indebtedness or (2) files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors.
- 9.3 In the event of expiration or termination of this Agreement or any Order Form for any reason other than OEM's material breach and subject to OEM continuing compliance with the terms and conditions of the Agreement: (i) this Agreement shall continue in full force and effect for a maximum of three years after the effective date of termination to the extent necessary for OEM to support existing End Users that have executed the End User Agreement for the remainder of their then current subscription terms as set forth in the applicable Cloud Service Schedule (the "Wind-Down Period"), and (ii) any Cloud Service Schedule issued under the Agreement shall not renew for an additional renewal period if such renewal period extends beyond the effective date of termination or expiration of this Agreement. During the Wind-Down Period, OEM shall remain authorized to order further Named Users for such existing End Users to be co-terminus with the then-current subscription term for such existing End Users until expiration of the Cloud Service Schedule. If the Agreement is terminated other than OEM's material breach, SAP may approach the End User directly about commencing a direct relationship with such End User or transferring such relationship to another SAP partner. In the event the Agreement, Cloud Service Schedule or any Order Form is terminated due to OEM's material breach, then SAP may elect for the Agreement to continue as described in subsection (i) above or may terminate the Agreement (including all Order Form(s) and Cloud Service Schedule issued hereunder) and SAP may approach the End User directly about commencing a direct relationship with such End User or transferring such relationship to another SAP partner. Termination or expiration of this Agreement shall not relieve OEM of its outstanding payment obligations existing at the time of such termination or expiration. Any fees previously paid by OEM are non-refundable. After the expiration of the Wind-down Period, OEM shall immediately cease (a) use of all SAP Materials and Confidential Information, and (b) to identify itself as an authorized OEM for SAP or otherwise affiliated in any manner with SAP. Additionally, the parties hereto agree that communications to End Users and any publications/press releases regarding such termination shall be mutually agreed upon, in writing, prior to distribution.
- 9.4 Notwithstanding SAP's right to terminate as set forth in Article 9.2 above, in the event of (i) any material breach of this Agreement, Cloud Service Schedule or any Order Form which is not cured within thirty (30) days after receipt of written notice from SAP; or (ii) a determination by SAP that continued use of the Cloud Service may result in harm to the Cloud Service (including the systems used to provide the Cloud Service) or other SAP customers, or result in a violation of law or regulations of the United States, E.U., Irish and other applicable jurisdictions or any applicable legal obligation or legal rights of another, in addition to any other remedies available at law or in equity, SAP will have the right immediately, in SAP's sole discretion, to remove any potentially offending End User Data from the Cloud Service, deactivate End User's user name(s) and password(s) and/or suspend access to the Cloud Service.
- 9.5 End User shall have the ability to access its End User Data at any time during a subscription term as specified under the applicable Cloud Service Schedule. Furthermore, upon reasonable request, End User may export and retrieve its End User Data during a subscription term, which request will be subject to technical limitations caused by factors such as (i) the size of End User's instance of the Cloud Service; and (ii) the nature of End User's request, e.g., the frequency and/or timing of the export and retrieval. End User shall have the ability to export and retrieve its End User Data within thirty (30) days after the effective date of termination. Thirty (30) days after the effective date of termination, SAP shall have no obligation to maintain or provide any End User Data. Except when such End User Data has been removed in accordance with Section 9.4, or exported by End User, upon termination of the Agreement, SAP shall use commercially reasonable efforts to permanently and irrevocably remove, purge or overwrite all data still remaining on the servers used to host the Cloud Service, including, but not limited to, End User Data, unless and to the extent applicable laws and regulations require further retention of such data.

- 9.6 Any terms of this Agreement which by their nature extend beyond the day this Agreement ends remain in effect until fulfilled, in particular any terms protecting the Intellectual Property Rights of an SAP Group Company, and apply to respective successors and assignees.
- 9.7 After the expiration of the Wind-down period, OEM shall irretrievably destroy or upon SAP's request deliver to SAP all copies of the SAP Materials and Confidential Information in every form, except to the extent it is legally required to keep it for a longer period in which case such return or destruction shall occur at the end of such period. OEM must certify to SAP in writing that it has satisfied its obligations under this Section.

## **10. IMPORT AND EXPORT CONTROLS**

- 10.1 The Cloud Service, Documentation and SAP Materials are subject to the export control laws of various countries, including without limit the laws of Ireland, United States and Germany. OEM agrees that it will not submit the Cloud Service, Documentation or other SAP Materials to any government agency for licensing consideration or other regulatory approval without the prior written consent of SAP. OEM agrees to comply with the laws and regulations restricting import, export, re-export, transfer or release to certain entities or destinations of the United States, E.U., Irish and other applicable jurisdictions ("Export Regulations"). With respect to any export, re-export, transfer, or release otherwise permitted under this Agreement to persons within OEM or its Affiliates or to unrelated third parties of: (i) such technology, software, services or commodities; or (ii) the direct product of any such technology; or (iii) any product that OEM creates with content that is supplied by SAP; or (iv) any technology that OEM creates that is based upon or commingled with technology provided by SAP, OEM will comply with the Export Regulations.
- 10.2 Any import into and/or operation in countries where the import and/or operation is subject to authorization by the authorities of such country shall be in the sole responsibility of OEM. SAP assumes no responsibility or liability for OEM's failure to obtain any necessary export approvals. OEM shall take all necessary actions and precautions to ensure that its distributors, resellers and other customers do not contravene the Export Regulations. SAP will reasonably cooperate with OEM to identify the export status and requirements of the Cloud Service or other SAP Materials. Notwithstanding anything to the contrary, SAP may refuse the fulfillment of its obligations under this Agreement if and for as long as such fulfillment violates the Export Regulations. The parties shall then consult each other if and how compliance with the Export Regulations may be achieved with commercially reasonable efforts. For the avoidance of doubt: SAP may request money for any modification of its Cloud Service that the parties may agree to, in their sole discretion, in order to make the item compliant. This Section 10 shall survive the expiration or earlier termination of this Agreement.
- 10.3 With respect to any provision of the Cloud Service, Documentation and SAP Materials to be made by SAP to OEM and/or any other party under this Agreement, OEM acknowledges that the provision of the Cloud Service, Documentation and SAP Materials may be subject to the prior obtaining of export and/or import authorizations from the competent authorities and that this process may considerably delay or prevent the delivery and/or impact SAP's ability to provide support. OEM shall support SAP in obtaining any required authorization by providing information and/or declarations, e.g. End Use Certificates, as may be requested by SAP.

## **11. OEM'S COMPLIANCE OBLIGATIONS**

- 11.1 OEM shall conduct its operations at all times in strict compliance with all applicable anticorruption laws including the US Foreign Corrupt Practices Act (FCPA), the U.K Bribery Act 2010, and SAP's then current local SAP Code of Business Conduct. Such obligation shall also apply to the OEM's subcontractors, Affiliates, resellers and distributors. If OEM has in place or adopts policies which establish similar standards to the SAP Code of Business Conduct, OEM may comply with its own policies to fulfil the requirements of this Section.
- 11.2 OEM shall not obtain on SAP's behalf or provide to SAP any information which is not legally available in the Territory, or which is procurement-sensitive, proprietary, or classified, where there is reason to believe that possession of such information is unauthorized, illegal, or unethical.
- 11.3 OEM shall not make, offer or promise any payments or gifts directly or indirectly to any employee of potential End Users. Any business entertainment offered to potential End Users must comply with the spirit and letter of the limits established in the relevant then current local SAP Code of Business Conduct.
- 11.4 OEM represents and warrants to SAP that OEM and any other person acting on the OEM's behalf have not directly or indirectly paid, offered or promised to pay, or authorized the payment of, and will not directly or indirectly pay, offer or promise to pay, or authorize the payment of any monies or gifts or anything of value to any employee or representative of an End User or prospect, or government official or employee, political party official or candidate, or officer or employee of any public international organization (or an immediate family member of such persons) for the purpose of influencing their acts or decisions in order to secure or retain business on behalf of SAP.
- 11.5 OEM represents and warrants that it is not listed by any government agency as debarred, suspended, or proposed for suspension or debarment or otherwise ineligible for government procurement programs. OEM certifies that neither it nor its employees or subcontractors are members of management or in a position to influence decisions related to work performed under this Agreement with respect to any End User.
- 11.6 SAP shall be entitled to require OEM to certify once per year that OEM is in compliance with the terms of this Section 11.

## **12. DATA PROTECTION**

- (i) OEM agrees to coordinate with the End Users for the execution of SAP's then-current CPPD Schedule, a current copy of which as of the date of this Agreement is attached hereto as Annex 1. SAP may, in its sole discretion, update the CPPD Schedule and/or make the most current version of the CPPD Schedule available to OEM online through an SAP-designated website, and OEM shall use such current version of the CPPD Schedule for the purposes described herein. For this purpose, OEM is hereby authorized to accept any CPPD Schedule from its End Users; provided



however that OEM is not authorized to negotiate and/or accept any amendments to the CPPD Schedule on behalf of SAP or any of its Group Companies.

- (ii) OEM agrees to promptly notify SAP of any CPPD Schedule executed by an End User and any subsequent terminations or expiration thereof and/or the terminations or expiration of SAP or its Group Companies' obligation to provide Cloud Services to such End Users.
- (iii) At SAP's request, OEM agrees to coordinate with the End User in the event SAP wishes to amend the CPPD Schedule or provide notice thereunder to the End User and to obtain the End Users' necessary consents or acceptance thereto on behalf of SAP, and to otherwise support SAP in this regard as SAP may reasonably request.
- (iv) OEM shall enter into appropriate data protection agreements with its End Users as required by applicable data protection laws.

### **13. MISCELLANEOUS**

- 13.1 **Assignment.** This Agreement may be assigned by SAP to any entity which assumes its obligations or acquires ownership of or the right to use and license the Software. Neither this Agreement, nor any right or obligation hereunder, may be assigned, transferred, delegated or subcontracted, by operation of law or otherwise, in whole or in part, by OEM without SAP's prior written consent, such consent not to be unreasonably withheld. Due to the importance of OEM's ownership and management, a Change of Control of OEM shall be deemed an assignment of this Agreement. "Change of Control" of OEM shall mean a transaction or series of transactions (i) pursuant to which Control of OEM is acquired by persons or entities other than those who Control OEM on the Effective Date of this Agreement, or (ii) resulting in the sale of all or substantially all of OEM's assets or all or substantially all of OEM's assets utilizing any Software or SAP Materials. Subject to the foregoing, the provisions of this Agreement shall be binding upon and inure to the benefit of the parties, and their permitted successors and assigns. OEM shall provide to SAP written notice at least sixty (60) days prior to any proposed assignment or transfer. Any attempted assignment or transfer of this Agreement is in violation of this Section is void.
- 13.2 **Independent Contractors.** The relationship of SAP and OEM established by this Agreement is that of independent contractors. This Agreement does not give either party the power to direct and control the day to day activities of the other, constitute the parties as partners, joint venturers, co-owners, principal-agent, or otherwise participants in a joint or common undertaking, or allow either party to create or assume any obligation on behalf of the other party for any purpose whatsoever. OEM has no actual, apparent, or ostensible authority to act on behalf of SAP unless expressly stated in this Agreement. OEM must indemnify and hold harmless SAP and its Group Companies in respect of any third party claims against SAP and/or any of its Group Companies arising or relating to a third party's assertion that the OEM acted as SAP's agent or otherwise on this behalf.
- 13.3 **Entire Agreement.** This Agreement constitutes the complete and exclusive statement of the agreement between SAP and OEM, and all previous representations, discussions, and writings are merged in, and superseded by this Agreement and the parties disclaim any reliance on any such representations, discussions and writings. Each party acknowledges that it is entering into this Agreement as a result of its own independent investigation and not as a result of any representation of the other party not contained herein. Any additional or different terms in OEM's documents (including any preprinted terms contained on purchase orders) are hereby deemed to be material alterations and notice of objection to, and rejection of, them is hereby given, and such additional or different terms shall be void. Signatures sent by electronic means (facsimile or scanned and sent via e-mail) shall be deemed original signatures.
- 13.4 **Amendments; Waivers.** This Agreement may not be modified or any term or condition waived except in a writing signed by a duly authorized representative of each party. This shall also apply to a possible waiver of the written form requirement established in the foregoing sentence. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provision hereof.
- 13.5 **Force Majeure.** Except for a party's payment obligations, neither party shall be liable to the other for its failure to perform any of its obligations hereunder during any period in which such performance is delayed by circumstances beyond its reasonable control including, but not limited to, earthquake, fire, flood, war, embargo, strike, riot, inability to secure materials and transportation facilities, or the intervention of any governmental authority.
- 13.6 **Publicity.** The terms of this Agreement are confidential. Except as otherwise set forth in this Agreement, no press release or other like publicity regarding this Agreement may be made without the other party's approval.
- 13.7 **Notices.** All notices or reports which are required or may be given pursuant to this Agreement shall be in writing and shall be deemed duly given when delivered to OEM or SAP at the addresses first set forth in this Agreement or applicable Order Form. Notices provided by OEM to SAP shall be sent to the attention of: SAP Legal Department. Where in this Section 13.7 or elsewhere in this Agreement notices in written form are required, that requirement can be met by facsimile transmission, email or exchange of letters to the address, email address or facsimile number of the respective parties set forth in any Order Form.
- 13.8 **Non-Exclusivity.** This is a non-exclusive relationship. Each party may have similar agreements with others and may independently develop, acquire, and market materials, equipment, or programs that may be competitive with (despite any similarity to) the other party's products or services. Each party is responsible for its own costs, including all business, travel and living expenses incurred by the performance of this Agreement.
- 13.9 **Hierarchy.** The following order of precedence (in descending order of priority) shall be applied in the event of conflict or inconsistency between provisions of the components of this Agreement: (i) Cloud Service Schedule, (ii) the Order Form or Addendum to the Agreement; (iii) the Exhibits; (iv) this Agreement (excluding applicable exhibits and schedules attached or referenced thereto) and (v) the Cloud GTC.

## 14. WARRANTIES AND DISCLAIMER

- 14.1 SAP warrants that the Cloud Service (excluding any third party products, content or services accessed through the Cloud Service) will substantially conform to the specifications stated in the Documentation during the applicable subscription term for such Cloud Service. The foregoing warranty shall not apply: (i) if the Cloud Service is not used in accordance with this Agreement, the Order Form, Cloud Service Schedule and/or any Documentation; or (ii) if the non-conformity is caused by third party services, content or products or any modifications, configurations or customizations to the Cloud Service; or (iii) to free (no fee) or trial licenses of the Cloud Service.
- 14.2 OEM shall report any non-conformities with respect to Section 14.1 to SAP in writing without undue delay through an SAP approved support channel, submitting a detailed description of the problem and any information useful for rectification of the non-conformity.
- 14.3 Provided OEM complies with Section 14.2 such that existence of non-conformity is validated, SAP will, at its option: (i) repair the non-conforming Service; or (ii) return an appropriate portion of any payment made by OEM with respect to the affected portion of the applicable Cloud Service. This is OEM's sole and exclusive remedy under this warranty.
- 14.4 EXCEPT AS EXPRESSLY PROVIDED IN SECTION 14.1, NEITHER SAP NOR ITS LICENSORS MAKE ANY REPRESENTATION OR WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, REGARDING ANY MATTER, INCLUDING THE MERCHANTABILITY, SUITABILITY, ORIGINALITY, OR FITNESS FOR A PARTICULAR USE OR PURPOSE, NON-INFRINGEMENT OR RESULTS TO BE DERIVED FROM THE USE OF THE CLOUD SERVICE, OR ANY INFORMATION TECHNOLOGY SERVICES, SOFTWARE, HARDWARE OR OTHER MATERIALS PROVIDED UNDER THIS AGREEMENT, OR THAT THE OPERATION OF ANY SUCH SERVICE, SOFTWARE, HARDWARE OR OTHER MATERIAL WILL BE UNINTERRUPTED OR ERROR FREE.
- 14.5 OEM represents and warrants that within industry standards it has and will maintain sufficient facilities and adequate capital, resources, and personnel to market and support the Bundled Service and to perform its obligations under this Agreement. Further, OEM represents and warrants that it will comply with all legal requirements applicable in the Territory and that it knows the essential functional characteristics of the Cloud Service and bears the risk that the Cloud Service does not meet OEM's or any End User's requirements.
- 14.4 OEM shall not make any representations or warranties as to the performance of the Cloud Services or other services on behalf of SAP or otherwise make commitments on behalf of SAP.

## 15. LIMITATION OF LIABILITY

- 15.1 ANYTHING TO THE CONTRARY HEREIN NOTWITHSTANDING, EXCEPT FOR DAMAGES RESULTING FROM UNAUTHORIZED USE OR DISCLOSURE OF CONFIDENTIAL INFORMATION AND SAP'S RIGHT TO COLLECT UNPAID FEES, UNDER NO CIRCUMSTANCES AND REGARDLESS OF THE NATURE OF ANY CLAIM SHALL EITHER SAP (OR ITS GROUP COMPANIES OR SAP'S LICENSORS) BE LIABLE TO OEM, ANY END USER OR ANY OTHER PERSON OR ENTITY FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE FEES PAID FOR THE APPLICABLE CLOUD SERVICE IN THE TWELVE (12) MONTH PERIOD PRECEDING THE DATE OF THE INCIDENT GIVING RISE TO LIABILITY AND UNDER NO CIRCUMSTANCES IN THE AGGREGATE FOR ALL CLAIMS TO EXCEED AN AMOUNT PAID TO SAP DURING TERM OF THIS AGREEMENT. UNDER NO CIRCUMSTANCES SHALL SAP, ITS GROUP COMPANIES OR SAP'S LICENSORS OR BE LIABLE IN ANY AMOUNT FOR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES, LOSS OF GOOD WILL OR BUSINESS PROFITS, WORK STOPPAGE, DATA LOSS, COMPUTER FAILURE OR MALFUNCTION, OR EXEMPLARY OR PUNITIVE DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
- 15.2 The provisions of this Agreement allocate the risks between SAP and OEM. The Cloud Service fees reflect this allocation of risk and limitations of liability herein. The aforementioned liability limitations shall include any claims against employees of, subcontractors of, or any other persons authorized by, SAP. Under no condition will SAP or its licensors be responsible under this Agreement for preparation or conversion of data into the form required for use with the Software.
- 15.3 OEM ACKNOWLEDGES THAT NONE OF SAP OR ITS LICENSORS ARE ENGAGED IN THE BUSINESS OF RENDERING LEGAL, TAX, OR OTHER PROFESSIONAL SERVICES AND THAT THE INFORMATION PROVIDED BY SAP RELATIVE TO THIS AGREEMENT OR IN RESPONSE TO OEM INQUIRIES ARE NOT INTENDED TO PROVIDE LEGAL, TAX OR OTHER EXPERT ADVICE TO OEM, OR BE A SUBSTITUTE FOR A LAWYER, ACCOUNTANT, OR OTHER PROFESSIONAL. IF OEM NEEDS LEGAL OR TAX ADVICE OR OTHER EXPERT ASSISTANCE, THE SERVICES OF A COMPETENT LAWYER, ACCOUNTANT, OR OTHER PROFESSIONAL LICENSED TO PRACTICE IN THE APPLICABLE JURISDICTION SHOULD BE SOUGHT.
- 15.4 The foregoing limitation of liability on direct damages only does not apply to personal injury or death caused by the gross negligence or willful misconduct of SAP, or tangible property damage (excluding data) up to the amount by which such damage is paid by SAP's liability insurance.
- 15.5 Claims. Neither party will bring a legal action under this Agreement more than two more than two years after the cause of action arose.
- 15.6 The parties expressly agree that should any limitation or provision contained in Sections 14 and 15 be held to be invalid under any applicable statute or rule of law it shall to that extent be deemed omitted but if either party thereby becomes liable for loss or damage which would otherwise have been excluded or limited such liability shall be subject to the other limitations and provisions set out herein.

## 16. GOVERNING LAW

This Agreement and any claims arising out of or relating to this Agreement and its subject matter shall be governed by and construed under the laws of Commonwealth of Pennsylvania without reference to its conflicts of law principles. In the

event of any conflicts between foreign law, rules, and regulations, and United States law, rules, and regulations, United States law, rules, and regulations shall prevail and govern. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement. The Uniform Computer Information Transactions Act as enacted shall not apply. The parties hereby submit to the exclusive jurisdiction and venue of the state and federal courts of the Commonwealth of Pennsylvania for all disputes arising from or in connection with this Agreement.

**17. SEVERABILITY; INJUNCTIVE RELIEF**

- 17.1 The terms of this Agreement are severable. If any term hereof is held invalid, illegal, or unenforceable for any reason whatsoever, such term shall be enforced to the fullest extent permitted by applicable law, and the validity, legality, and enforceability of the remaining terms shall not in any way be affected or impaired thereby.
- 17.2 Both parties acknowledge that remedies at law may be inadequate to provide SAP or OEM with full compensation in the event of OEM's material breach of Sections 7.2 or 7.4 with respect to SAP's Confidential Information and its Trademarks or SAP's material breach of Section 7.4 with respect to OEM's Confidential Information, and that the non-breaching party shall therefore be entitled to seek injunctive relief in the event of any such material breach, without posting a bond.

**ANNEX 1**  
**SAP OEM Cloud Service Schedule**  
**for Commissioned Processing of Personal Data**

**SAP OEM Cloud Service Schedule**  
**For Data Privacy And Security**

**Effective [ date ] (“Effective Date”)**

**Business Objects Software Limited**  
**1012 - 1014 Kingswood Avenue**  
**City West Business Campus**  
**Dublin 24, Ireland**  
**(hereinafter “SAP”)**

represented through:

**OEM Named:** \_\_\_\_\_ (“OEM”)

and

**Customer Name:** \_\_\_\_\_

**Customer Address:** \_\_\_\_\_  
**(hereinafter “Customer”)**

**PREAMBLE:**

WHEREAS Customer has entered into an agreement (“End User Agreement”) with [Name of Partner] (“OEM”) for the supply of and was granted the right to use the SAP Cloud Service as set out in the applicable Order Form (“Order Form”) submitted by OEM to SAP (“Service”) solely in conjunction with OEM’s own hosted, on-demand services (“Partner Services”);

WHEREAS OEM has entered into an OEM license agreement for Cloud Service or OEM Order Form for Cloud Service (collectively, “OEM Agreement”) with SAP whereby SAP grants to OEM the right to promote, market and resell SAP Cloud Service solely in conjunction with Partner Services;

WHEREAS Customer desires to grant consent to SAP for the processing of personal data by SAP on behalf of Customer and its Affiliates and their respective employees, agents, contractors, consultants, suppliers or other individuals who are authorized by Customer to use the SAP Cloud Service (“Named Users”); and

WHEREAS SAP accepts to provide for an adequate level of data protection and security through the contractual obligations set forth in this Exhibit and any attachments referred herein; and

WHEREAS Customer understands and acknowledges that OEM, through which Customer has arranged for the procurement of the SAP Cloud Service or from which Customer receives any services related to the SAP Cloud Service, is not an agent of SAP.

NOW, THEREFORE, and in consideration of good and valuable consideration, the receipt of which is hereby acknowledged, the Parties agree as follows:

SAP and Customer agree that this OEM Cloud Service Exhibit for DATA PRIVACY AND SECURITY stipulates the rights and obligations of Customer and SAP in connection with personal data processed by SAP on behalf of Customer and its Affiliates for the Named Users under the Order Form solely for the Cloud Service (but excluding any Partner Services). References to “Affiliates” means party means any legal entity in which a party, directly or indirectly, holds more than fifty percent (50%) of the shares or voting rights or controls or is under common control with that legal entity. “Control” means the direct or indirect possession of the power to direct or cause the direction of the management and policies of an entity, whether through ownership, by contract or otherwise. Any such company shall be considered an Affiliate for only such time as such interest or control is maintained.

This Exhibit shall become an integral part of the End User Agreement. Any capitalized terms referenced herein shall have the meaning given to them in the End User Agreement. This Exhibit in conjunction with its Appendices stipulates:

- a) the rights and obligations of Customer and SAP in connection with personal data that SAP and its authorized Subprocessors process on behalf of Customer and its Affiliates pursuant to the Agreement; and
- b) the applicable technical and organizational measures SAP implements and maintains to protect Customer Data

**1. Definitions**

“Data exporter” as defined in the Standard Contractual Clauses shall mean Customer as listed in an Order Form or its respective Affiliates.

“Data importer” as defined in the Standard Contractual Clauses shall mean the applicable Non EU Entity.

“Non EU Entity” means any SAP entity or Subprocessor incorporated in a country which does not provide for an adequate level of data protection according to European Union (EU) laws and regulations.

“Standard Contractual Clauses” shall mean the (Standard Contractual Clauses (processors)) based on the Commission Decision of 5 February 2010, on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (notified under document number C(2010) 593) including Appendices 1 and 2 attached hereto.

“Subprocessor” as defined in the Standard Contractual Clauses shall mean the SAP Affiliates or third party subprocessors engaged by SAP in accordance with section 5 below.

**2. Data Processing Purposes**

2.1 Customer and its Affiliates, as the respective data controller(s), shall determine the purposes of collecting, processing, and otherwise using personal data stored in the Service. Unless provided otherwise in a product supplement or Order Form, Appendix 1 of the Standard Contractual Clauses attached hereto shall apply to such data processing.

2.2 The purposes for processing personal data stored in the Service or otherwise provided to SAP and its Affiliates under the End User Agreement are limited to:

- a) Setting up, operating, monitoring and providing the Service, including the underlying infrastructure (hardware, software, secure data center facilities, connectivity), as a data processor or Subprocessor in accordance with the agreed System Availability as defined in the Agreement;
- b) Providing technical support as a main obligation of SAP under the End User Agreement;
- c) Providing professional services as a main obligation of SAP, if and to the extent agreed by the parties.

### 3. Standard Contractual Clauses, Limitations of Liability and Applicable Laws

3.1 The unchanged version of the Standard Contractual Clauses shall be deemed incorporated by reference hereto and apply if and to the extent a Non EU Entity (a) can remotely access or process personal data of Customer and its Affiliates that SAP hosts in an EU based data center; or (b) hosts personal data from Customer or Customer Affiliate(s) who are incorporated in a member state of the EU/EEA or Switzerland in a data center outside the EU. Unless otherwise agreed by the parties, Appendix 1 and 2 of the Standard Contractual Clauses as attached shall apply. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses if and to the extent applicable to the data processing outside the EU by SAP and its authorized Subprocessors. Customer acknowledges it has had the opportunity to review the Standard Contractual Clauses or to obtain a full copy from SAP.

3.2 A new paragraph 4 shall be added to Clause 6 (Liability) to the Standard Contractual Clauses to read:

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon:

- (a) the data exporter promptly notifying the data importer of a claim; and
- (b) the data importer being given the possibility to cooperate with the data exporter in the defense and settlement of the claim.

3.3 SAP may, in its sole discretion, update or replace the Standard Contractual Clauses by an alternative means (e.g., binding corporate rules) deemed adequate under the then-current EU data protection regulations by providing Customer with thirty (30) days prior written notice (email permitted) thereof.

3.4 Notwithstanding the foregoing, the liability of SAP shall be limited to damages directly caused by the culpable conduct of its own and its authorized Subprocessors processing operations in breach of its obligations set forth in this Exhibit. SAP AND ITS AFFILIATES DISCLAIM ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT EXCEPT TO THE EXTENT THAT ANY WARRANTIES IMPLIED BY LAW CANNOT BE VALIDLY WAIVED.

3.5 More stringent laws may apply directly to the parties under its local applicable data privacy laws and regulations. This Exhibit is not meant to reduce the level of protections applicable to each data subject. In the event and to the extent of any conflict between the terms and conditions of this Exhibit and applicable law, the provision(s) of applicable law shall govern to the fullest extent concerned.

### 4. SAP Obligations

4.1 SAP shall process personal data and other operating data of Customer and its Affiliates as provided to SAP by Customer, which may include (without limitation) the correction, erasure and/or the blocking of such data if and to the extent the functionality of the Service does not allow the Customer or Named User to do so. SAP shall notify Customer if SAP considers an instruction given by Customer on behalf of the data controller to be in violation of data protection laws. SAP shall not be obligated to perform a comprehensive legal examination.

4.2 For processing Customer Data, SAP shall only use personnel who have demonstrably committed themselves to observe data secrecy and secrecy of telecommunications pursuant to the applicable data protection laws. SAP shall use commercially reasonable efforts to ensure that those employees to whom it grants access to Customer Data are regularly trained on IT security and data protection.

4.3 SAP shall implement all technical and organizational measures to comply with requirements pursuant to applicable data protection laws. SAP undertakes to Customer that it has taken and will, on a continuing basis, take appropriate technical and organizational measures to keep Customer Data secure and protect it against unauthorized or unlawful processing and accidental loss, destruction or damage. In particular, SAP shall take and regularly check the following protection measures, as further described in Appendix 2:

- a) Physical access control: SAP shall install an access control system.
- b) Access control: SAP shall control and log access to data processing systems.
- c) Access limitation control: SAP shall define, implement and monitor a concept for user rights, rules for passwords and login procedures to remotely or physically access the Service by its personnel, as required to operate, maintain, support or secure the Service.
- d) Transmission control: SAP shall ensure Customer Data transmission in encrypted form or by a secure alternative procedure. Transmissions must be logged and guidelines for Customer Data transmissions must be laid down in writing.
- e) Input control: SAP shall implement a detailed logging system for input, modification and deletion or blocking of Customer Data to the greatest extent supported by the Service.
- f) Job control: SAP shall define in writing and establish control mechanisms to ensure that Customer Data is processed strictly in accordance with the instructions of the data controller as provided to SAP by Customer and as contemplated in the End User Agreement.
- g) Availability control. SAP shall run a state of the art backup system and define a restore operation procedure to protect Customer Data from accidental destruction or loss.
- h) Data separation: SAP shall ensure by technical means and defined organizational procedures that Customer Data collected for different purposes (e.g., different customers) can be processed separately. Technical means can be separated computer systems or demonstrably logical separation in a multi-tenant architecture. Access by one SAP customer to the data of any other SAP customer must be prevented.

Since SAP provides the Service to all customers uniformly via a hosted, web-based application, all appropriate and then current technical and organizational measures apply to SAP's entire customer base hosted out of the same data center and subscribed to the same Service. Customer understands and agrees that the technical and organizational measures are subject to technical progress and development. In that regard, SAP is specifically allowed to implement adequate alternative measures as long as the security level of the measures is maintained. In the event of any significant changes SAP shall provide a notification together with any necessary documentation related thereto to Customer by email or publication on a website easily accessible by Customer.

4.4 If SAP determines that the security measures implemented by SAP do not meet the legal requirements, SAP shall promptly notify Customer.

4.5 SAP shall promptly inform Customer in the event of serious disruptions of the operating process, suspected data protection violations or other irregularities in connection with the processing of Customer Data.

4.6 At Customer's written request and at Customer's expense, SAP shall reasonably support Customer in dealing with requests from individual data subjects and/or a supervisory authority with respect to the processing of personal data hereunder. SAP shall notify Customer about inspections and measures of a supervisory or other competent authority.

## 5. Subprocessors

Customer hereby authorizes SAP (also in accordance with Clause 11 paragraph 1 of the Standard Contractual Clauses) to engage subcontractors for the processing of personal data (each a "Subprocessor") to the extent necessary for fulfilling its contractual obligations under the End User Agreement as long as SAP remains responsible for any acts or omissions of its Subprocessors in the same manner as for its own acts and omissions hereunder. SAP shall pass on to Subprocessors SAP's obligation as data processor vis-à-vis Customer as set out in this Exhibit and obligate Subprocessors to obey all relevant data protection rules. SAP will inform Customer upon its request by email or through a web site accessible to Customer about the name, address and role of each Subprocessor. SAP may remove or appoint suitable and reliable Subprocessors at its own discretion. SAP will inform Customer by email or otherwise in advance of any changes to the list of Subprocessors. If Customer has a legitimate reason to object to SAP's use of a Subprocessor Customer shall notify SAP thereof in writing within thirty (30) days after receipt of SAP's notice. If Customer does not object during such time period the new Subprocessor(s) shall be deemed accepted. If Customer objects to the use of the Subprocessor concerned SAP shall have the right to either provide the Service without such Subprocessor or to terminate the End User Agreement for the Cloud Service only with thirty (30) days prior written notice. In any event, SAP shall ensure that each Subprocessor adheres to an adequate level of data protection by law or contract not materially less protective than the obligations applicable to SAP under the End User Agreement. In case that such Subprocessor is located outside the EU, SAP shall provide for a level of data protection deemed adequate under EU data protection regulations.

## 6. Monitoring Rights of Customer

6.1 Unless otherwise provided in a supplement or Order Form, during the term of the Agreement, Customer may request an annual written self-certification from SAP based on an independent third party audit that scrutinizes and confirms the processing of Customer Data is in accordance with the agreed to measures herein. If SAP fails to perform its audit obligations hereunder, Customer (or an independent third party auditor on its behalf that is subject to confidentiality obligations consistent with those in the Agreement) may audit SAP's control environment and security practices relevant to personal data processed hereunder once in any twelve (12)-month period, with reasonable prior written notice (at least 60 days) and under reasonable time, place and manner conditions.

6.2 SAP shall reasonably support Customer throughout these verification processes and provide Customer with the required information. Customer shall bear any costs (including SAP's internal resource based on then-current daily professional service rates per SAP's price list) exceeding more than 4 hours per year.

## 7. General Provisions.

7.1 Customer may not, without SAP's prior written consent, assign, delegate, pledge, or otherwise transfer this Exhibit, or any of its rights or obligations under this Exhibit, to any party, whether voluntarily or by operation of law, including by way of sale of assets, merger or consolidation. SAP may assign this Exhibit to its Affiliates.

7.2 If any provision of this Exhibit is found by any court of competent jurisdiction to be invalid or unenforceable, the invalidity of such provision shall not affect the other provisions of this Schedule, and all provisions not affected by such invalidity shall remain in full force and effect.

7.3 Any notice required or permitted to be given hereunder shall be deemed sufficient if made in writing (email permitted) and delivered to the respective executive offices of SAP or Customer at the address first set forth above.

7.4 Any delay or nonperformance of any provision of this Exhibit caused by conditions beyond the reasonable control of SAP shall not constitute a breach of this Exhibit, and the time for performance of such provision, if any, shall be deemed to be extended for a period equal to the duration of the conditions preventing such performance.

7.5 This Exhibit and any disputes arising out of or in connection with this Exhibit shall be governed by and construed in accordance with the laws of the country of Customer's place of business stated above in this Exhibit.

7.6 This Exhibit constitutes the complete and exclusive statement of the agreement between SAP and Customer, and all previous representations, discussions, and writings are merged in, and superseded by this Exhibit. No modifications, amendments, or supplements to this Schedule shall be effective for any purpose unless in writing and signed by the parties. Although SAP has authorized Partner to execute this Exhibit as part of the End User Agreement with Customer, Customer's rights and SAP's obligations hereunder are limited to the unchanged version of the Exhibit as provided by SAP to Partner or as published by SAP on its website.

Accepted by:

Customer: [\_\_\_\_\_]

Authorized Signature: \_\_\_\_\_

Type Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## **APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES AND EXHIBIT 1**

**The parties may provide further details in an Order Form, if required.**

### **Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporter subscribed to certain SAP Cloud Services which allow its Named Users to enter, amend, use, delete or otherwise process Customer Data as contemplated under the End User Agreement.

### **Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

SAP and its Subprocessor provide certain Cloud Services which include the hosting of the Service and the provision of technical support to Customer, its Affiliates and their respective Named Users as contemplated under the End User Agreement.

### **Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

Unless provided otherwise by data exporter, data subjects may include employees, contractors, business partners or other individuals whose personal data is stored in the Service.

### **Categories of data**

The personal data transferred concern the following categories of data (please specify):

Customer determines the categories of data per Service subscribed. Customer's data fields can be configured as part of the implementation of the Service or as otherwise permitted in the Service. The personal data transferred usually concern (a subset of) the following categories of data: name, phone numbers, e-mail address, time zone, company name, company address data, plus any application-specific data which Customers' Named Users enter into the Service.

### **Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

Not permitted (unless Customer has otherwise notified SAP)

### **Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

- use of Customer Data to provide the Service and to provide assistance to technical support
- storage of Customer Data in dedicated Service data centers (multi-tenant architecture)
- upload any patch, update, upgrade / new releases to the Service
- back up of Customer Data
- computer processing of Customer Data, including data transmission, data retrieval, data access
- network access to allow Customer Data transfer, if required

## **APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES AND EXHIBIT 1**

Some Cloud Services are subject to different technical support terms, as set forth in the respective Supplement or Order Form.

In all other cases, the description of the technical and organizational security measures (TOMs) implemented by the data importer for Customer Data in accordance with Clauses 4(d) and 5(c) shall apply:

### **A. TOMs: Cloud Service**

#### **1. Access Control**

*Aim: Prevent any unauthorized access; the term is interpreted literally to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data.*

Measures: Technical and organizational measures for access control, especially to control the legitimacy of authorized entrants to the facilities and systems where data is stored.

SAP takes measures to secure the hosting premises (for example, securing entries and exits) as well as measures within the building (for example, alarm systems and restricted access to server rooms) at rented facilities through the use of the following procedures:

- established security areas;
- protection and restriction of access paths;
- secured the decentralized data processing equipment and personal computers;
- established access authorizations for employees, including the respective documentation;
- identification of the persons having access authority;
- regulations on key-codes;
- restriction on keys;
- code card passes;
- visitors books (including timekeeping);
- security alarm system or other appropriate security measures.

#### **2. System Access Control**

*Aim: Prevent unauthorized intrusion into computer systems.*

Measures: Technical (password / password protection) and organizational (user master record) measures concerning the user identification and authentication:

- SAP employs industry standard encryption.
- User control shall include the following measures:
  - restricted VPN profile;
  - automatic turn-off of the user ID when several erroneous passwords are entered, log file of events (e.g., monitoring of break-in-attempts);
  - issuing of one-time use password controls;
  - implementation of 2-factor authentication
- Access control to Customer Data shall include the following measures:
  - monitoring capability in respect of individuals who delete, add or modify the exported data;
  - automatic, system-driven reminders of the confidentiality appearing upon each attempt to access systems used in processing data;
  - effective and measured disciplinary action against individuals who access data without authorization.

#### **3. Data Access Control**

*Aim: Prevent unauthorized activities in computer systems resulting from the exceeding or bypassing of granted permissions. In particular, ensure that persons authorized to use a system have access only to those data they are authorized to access and that personal data cannot be read, copied, altered or removed without authorization during processing, use or after recording.*

Measures: Demand-driven design approach and the authorization of access rights, their monitoring and logging through the following:

- SAP uses a combination of segregation of duties, local access control lists, and central logging to ensure data is accessed as authorized and used in an appropriate manner:
  - Intrusion detection systems are installed on both the network and host systems to ensure appropriate access;
  - Access controls are reviewed on a periodic basis by both internal and external audits.
- SAP uses non-persistent session cookies for authentication and navigation purposes for a user's session, only.
- SAP employs industry standard encryption.

#### **4. Data Transmission Control**

*Aim: Define aspects of data transfer, data transport and transmission control. Ensure that data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media.*

Measures: used in transport, transfer and transmission or storage to disk (manual or electronic) as well as during subsequent controls:

This shall include measures jointly implemented by Customer and SAP comparable to the following:

- documentation of the retrieval and transmission programs;
- use of encryption;
- monitoring of the completeness and correctness of the transfer of data (success/failure reports will be sent to administrator).

#### **5. Data Input Control**

*Aim: Ensure the traceability and documentation of data management and maintenance. It should be possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and, if so, by whom.*

Measures: Methods used for subsequent review to reflect whether and by whom data were entered, modified or removed (deleted):

- This shall include measures comparable to the following:
  - proof established within the SAP's organization of the input authorization;



- o electronic recording of entries (as further specified by SAP).

## 6. Job control

*Aim: Ensure that the instructions of Customer are fully observed.*

Measures (technical / organizational) on the division of responsibilities between SAP and Customer:

- clearly defined responsibilities;
- criteria for selection of SAP, as determined and communicated by Customer;
- monitoring of execution and performance by reviews of the provided self-certification and audit, as applicable;
- named contacts for submission of change orders.

## 7. Availability Control

*Aim: Protect the data against accidental destruction or loss.*

Measures: For data storage/backup (physical / logical):

- documented daily incremental/weekly full backup procedures;
- redundant system infrastructure, Highly-Available Oracle clustering;
- uninterruptible power supply (UPS);
- separate storage;
- antivirus / firewall;
- emergency plan.

## 8. Separation control

*Aim: Data collected for different purposes can be processed separately.*

Measures for separate processing (storage, modification, deletion, transfer) of information with different purposes:

- functional separation / production / non-production: SAP maintains completely physical separation between production, development and testing. Customer is provisioned 2 distinct instances: one for production and at least one for non production.
- Customer (including its Affiliates) have access only to Customer's instance(s).

## B. TOMs: Cloud Support (separate SAP global support tracking system)

The following sections define the current security measures. SAP may improve or increase these at any time. This may mean that individual measures are replaced by new measures that serve the same purpose.

### 1. Access Control

*Aim: Prevent any unauthorized access; the term is interpreted literally to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data.*

Measures: SAP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.

- In general, buildings are secured through access control systems (smart card access system). As a minimum requirement, the outermost shell of the building must be fitted with a certified master key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises will be further protected by additional measures: These include specific access profiles, closed circuit TV, intruder alarm systems, and even biometric access control systems. A separate access control concept, which includes documentation of names, is used data centers.
- Access rights will be granted to authorized persons on an individual basis according to the defined criteria. This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception, and must be accompanied by company personnel.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

### 2. System Access Control

*Aim: Prevent unauthorized intrusion into computer systems.*

Measures:

- Multiple authorization levels are used to grant access to sensitive systems. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
- All users access SAP's system with a unique identifier (user ID).
- SAP has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, these access rights are rescinded.
- SAP has a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, and requires passwords to be changed on a regular basis. Personalized user IDs are assigned for authentication. All passwords are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months. This complies with the requirements for complex passwords. SAP ensures that default passwords are changed on networking devices. Each computer has a password protected screensaver.
- The company network is protected from the public network by a hardware firewall. SAP uses antivirus software at access points to the company network (for e-mail accounts) and on all file servers and all workstations.
- Security-relevant updates for the existing software are regularly and automatically downloaded and installed.

### 3. Data Access Control

*Aim: Prevent unauthorized activities in computer systems resulting from the exceeding or bypassing of granted permissions. In particular, ensure that persons authorized to use a system have access only to those data they are authorized to access and that personal data cannot be read, copied, altered or removed without authorization during processing, use or after recording.*

Measures:

- Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. SAP uses authorization concepts that document how authorizations are assigned and which authorizations are assigned. All personal, confidential, or otherwise sensitive data is protected in accordance with the relevant security standards. Confidential information must be processed confidentially.

- All production servers are operated in the relevant data centers/server rooms. The security systems that protect applications for processing personal, confidential or other sensitive data are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on the IT systems.
- SAP does not allow the installation of personal software or other software not approved by SAP.
- An SAP security standard governs how data and data carriers that are no longer required are deleted or destroyed.

#### **4. Data Transmission Control**

*Aim: Define aspects of data transfer, data transport and transmission control. Ensure that data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media.*

Measures: Data that is transferred from the SAP network to other external networks is encrypted. Where data carriers are physically transported, adequate measures must be taken to ensure the agreed service levels (for example, encryption, lead-lined containers, and so on).

#### **5. Data Input Control**

*Aim: Ensure the traceability and documentation of data management and maintenance. It should be possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and, if so, by whom.*

Measures: SAP only allows authorized persons to access personal data as required in the course of their work. As part of the support delivery process, the access to customer systems by users and administrators is recorded in a log file.

#### **6. Job Control**

*Aim: Ensure that the instructions of Customer are fully observed.*

Measures:

- SAP uses controls and processes to ensure compliance with contracts between SAP and its service providers.
- As part of the SAP security policy, no customer information is classified lower than “confidential”.
- Access to customer data systems is usually granted via remote support. This is governed by the following security requirements:
- In general, the remote internet connection is established via a Secure Network Communications (SNC) or Virtual Private Networks (VPN) connection. Both options use various security measures to protect customer systems and data from unauthorized access: These include strong encryption, user authentication, and access control technology.
- The Secure Area is a specially designated support ticket facility in which SAP provides a special access-protected and monitored security area for transferring the access data and password.
- At all times, SAP customers have control over their remote support connections. SAP employees cannot access a customer system without the knowledge or full active support of the customer.
- All SAP employees and contractual partners are contractual bound to respect the confidentiality of all sensitive information including information about the trade secrets of SAP customers and partners.
- During the support process, the personal data of different customers is physically or logically separated.

#### **7. Availability Control**

*Aim: Protect the data against accidental destruction or loss.*

Measures: SAP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary. SAP also uses uninterrupted power supplies (UPS, batteries, generators, and so on) to ensure power is available to the data centers. Emergency processes and systems are regularly tested.

Firewalls or other network security technologies are also used. In accordance with the security policy, regularly updated antivirus products are also available on all systems.

#### **8. Separation control**

*Aim: Data collected for different purposes can be processed separately.*

Measures for separate processing (storage, modification, deletion, transfer) of information with different purposes: Support tracking system separate from the Service.