

**- ePaaS Licensing of SAP Cloud Service Schedule -  
to the Platform Application Development Cooperation Agreement**

This Schedule consists of the Exhibits K-1, K-2, K-3, and Annex 1, and is hereby annexed to and made a part of the Platform Application Development Cooperation Agreement.

The SAP Cloud Service is provided under the terms and conditions of the Agreement supplemented with the following terms and conditions. In case of conflicting terms, the terms of this Schedule shall prevail.

**Exhibit K-1  
- ePaaS Licensing of SAP Cloud Service -  
to the Platform Application Development Cooperation Agreement**

This Exhibit K-1 to the Agreement between Partner and SAP stipulates the terms of licensing SAP Cloud Service available to Partner for sublicensing to End User as part of a Bundled Cloud Service.

Partner is entitled to use the SAP Cloud Service as outlined in this Schedule, and according to licensing and use restrictions as set forth in the Agreement. SAP will make available to Partner an Order Form which must be filled out and submitted to SAP for using the SAP Cloud Service as Bundled Cloud Service.

**1. DEFINITIONS**

All capitalized terms shall have the meaning ascribed in this Agreement.

- 1.1 "Bundled Cloud Service" ("BCS") means the combined offering of SAP Cloud Service and Cloud Application.
- 1.2 "Data" means any content, materials, data and information that is entered into the SAP Cloud Service.
- 1.3 "End User Agreement" means a written agreement entered into between Partner and any End User pursuant to which the End User purchases cloud subscriptions to the Bundled Cloud Service.
- 1.4 "Public Software" means any software, documentation or other material that contains, or is derived (in whole or in part) from, any software, documentation or other material that is distributed as free software, open source software (e.g., Linux) or similar licensing or distribution models, including, but not limited to software, documentation or other material licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (i) the GNU General Public License (GPL), Lesser/Library GPL (LGPL), or Free Documentation License, (ii) The Artistic License (e.g., PERL), (iii) the Mozilla Public License, (iv) the Netscape Public License, (v) the Sun Community Source License (SCSL), (vi) the Sun Industry Standards License (SISL), and (vii) the BSD License.
- 1.5 "SAP Cloud Service" means, for the purpose of this Schedule, SAP Cloud Service made available by SAP under this Agreement, signed-up to by Partner, to operate the Cloud Application only for use in conjunction with, and for purposes of provision and support of, Cloud Application to End User.
- 1.6 "SAP Materials" means any software, programs, tools, systems, data, or other materials made available by SAP to Partner prior to or in the course of the performance under this Agreement including, but not limited to, the SAP Cloud Service and Documentation, as well as any information, materials or feedback provided by Partner to SAP relating to the SAP Cloud Service and Documentation.

**2. GRANT OF RIGHTS**

- 2.1 Grant of SAP Cloud Service subscription license. Subject to the terms of this Agreement, SAP grants Partner during the term of the Agreement (and during any Wind-Down Period) a worldwide, non-exclusive, limited, non-transferable, non-sublicensable, non-perpetual right to use the SAP Cloud Service to operate the Cloud Application only for use in conjunction with, and for purposes of provision and support of, Cloud Application to End User, only available to Partner if (i) Partner has subscribed to the Innovation Pack for SAP HANA Cloud Platform as well as the respective additional SAP Cloud Service subscription for developing and supporting the Cloud Application under the Agreement, and if (ii) Partner is exclusively offering its BCS to End User as a cloud subscription offering under the Agreement. Partner shall not license, resell, rent, lease or otherwise provide any access or benefits to the SAP Cloud Service except for the provision of Partner's Cloud Application to its End Users.
- 2.2 BCS. Partner shall impose on the End Users the following restrictions: the End User Agreement shall permit the End User's use of the BCS, with data access limited to data created by the Cloud Application or necessary to enable the functionalities of the Cloud Application (referred to as a "Restricted License"). The SAP Cloud Service shall not access, directly or indirectly, in any manner whatsoever, any third party runtime database acquired from SAP or its Affiliates or any of its respective resellers or distributors. The BCS may access any other Licensor software, and/or third party software licensed from Licensor or Group Companies or any of its respective resellers or distributors, on a business process layer, e.g. via APIs, SAP HANA Cloud Integration, etc. Partner 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. Partner may operate the BCS, 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 operate the technology or service of such third-party supplier.

### 3. USE OF THE SAP CLOUD SERVICE

#### 3.1 GENERAL USE RIGHTS

- (a) Notwithstanding anything to the contrary provided in the Agreement, Partner and its End Users shall have access only to the most current version of the SAP Cloud Service made generally available by SAP to its customers, and SAP may change or modify the SAP Cloud Service at any time. SAP shall not materially diminish the functionality of the SAP Cloud Service Subscription during the term of the respective Purchase Order.
- (b) If the BCS is integrated with any SAP solution, End User must have the proper licenses for such SAP solution in order to access the SAP solution through the BCS. Fees for such licenses are not included in the fees for the SAP Cloud Service under the Agreement.
- (c) Partner will protect the privacy and legal rights of its End Users under all applicable laws and regulations, which includes a legally adequate privacy notice communicated from Partner (or to the extent applicable, obtain necessary consent according to data protection laws). Partner may have the ability to access, monitor, use, or disclose content, data and materials submitted by End Users through the Cloud Application. Partner will obtain and maintain any required consents from End Users to allow Partner's access, monitoring, use or disclosure of such content, data and materials. Further, Partner will notify its End Users that any information provided as part of the Cloud Application will be made available to SAP as part of SAP providing the SAP Cloud Service.
- (d) If SAP is notified by an End User or an owner of User Content that the User Content allegedly infringes its rights, SAP may investigate the allegation (including by consulting with Partner) and determine in good faith and in its reasonable discretion whether to remove the User Content, which it may do after providing Partner with prior notice regarding such removal within a reasonable time in light of the circumstances. SAP has no obligation to monitor User Content and interactions between End Users or Partner and its End Users. Partner shall take down any and all User Content of which it becomes aware that is infringing in a prompt manner or promptly notify SAP to do so.
- (e) Partner may not use the SAP Cloud Service, BCS, or any Cloud Application to generate, distribute, publish or facilitate unsolicited mass email, promotions, advertisements or other solicitations ("spam").
- (f) Partner shall not license, resell, rent, lease or otherwise provide any access to, or benefits to any third parties of the SAP Cloud Service except for the provision of Partner's Cloud Application to its End Users. Neither Partner nor any End User may run any third party application (other than Partner's Cloud Application) on the SAP Cloud Service, including without limitations, any application made available and published by SAP or its Affiliates on designated SAP digital properties. Use of SAP Cloud Service by End Users is limited to communications and data exchange between the Cloud Application or any other SAP Cloud Service, and the SAP Cloud Service via officially supported SAP Cloud Service interfaces. All data loading, modeling, reporting and distribution, creation and extension of tables used in SAP Cloud Service must be performed via the Cloud Application.
- (g) Partner shall not, and shall ensure that its End Users do not: (i) copy, translate, disassemble, decompile, reverse-engineer or otherwise modify any parts of the SAP Cloud Service; (ii) transmit any content, data or information that is unlawful, abusive, malicious, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another's privacy or right of publicity, hateful, or racially, ethnically or otherwise objectionable; (iii) infringe the intellectual property rights of any entity or person; (iv) interfere with or disrupt the SAP software or SAP systems used to host the SAP Cloud Service, or other equipment or networks connected to the SAP Cloud Service; (v) use the SAP Cloud Service in the operation of a service bureau, outsourcing or time-sharing service except as expressly permitted under this Agreement; (vi) circumvent or disclose the user authentication or security of the SAP Cloud Service or any host, network, or account related thereto; (vii) make any use of the SAP Cloud Service that violates any applicable local, state, national, international or foreign law or regulation.
- (h) SAP shall have the right to monitor any Partner and its End Users' usage of the SAP Cloud Service to ensure compliance by Partner and its End Users of the Agreement. Subject to SAP's confidentiality obligations under this Agreement, SAP may utilize the information concerning Partner or its End Users' usage of the SAP Cloud Service to improve SAP products and services and to provide Partner with reports on its End Users' use of the SAP Cloud Service.
- (i) Partner and its End Users shall be responsible for entering its Data into the SAP Cloud Service and Partner and the End Users shall be responsible for the content of the Data supplied by it, as the case may be. Partner agrees that it has collected and shall maintain and handle all Data whether originated by Partner or its End Users in compliance with all applicable data privacy and protection laws, rules and regulations. Partner shall maintain commercially reasonable security standards for its and its End Users' use of the SAP Cloud Service.
- (j) SAP may offer and Partner may choose to accept access to functionality that is not generally available and not validated and quality assured in accordance with SAP's standard processes ("Beta Functionality"). Beta Functionality is described as such in the Documentation. SAP may require Partner to accept additional terms to use Beta Functionality. Any production use of the Beta Functionality is at Partner's sole risk. SAP does not warrant the correctness and completeness of the Beta Functionality, and SAP shall not be liable for errors or damages caused by the usage of the Beta Functionality.
- (k) The SAP Cloud Service may contain links to external Web sites (including embedded widgets or other means of access) and information provided on such external websites by SAP partners and third-party service providers. SAP shall not be responsible for the contents of any linked Web site, or any changes or updates to such sites.

Partner further agrees that SAP shall not be directly or indirectly responsible or liable for any damage or loss caused or alleged to be caused by or in connection with Partner's use of or reliance on any content, goods or services available on or through any such linked Web site. Any article, information, data, code, text, software, documentation, graphics, image, marketing material, video, photograph, message, or posting to any forum, wiki, or blog access through or in connection with the SAP Cloud Service, whether publicly posted or privately transmitted (collectively, "Content"), is the sole responsibility of the person or entity providing the content.

- (l) SAP will release updates to SAP Cloud Service as required for the security and stability of the system. Partner should support these updates in order to prevent the possibility of loss of data or the instability of the platform. If Partner does not support these upgrades in the recommended time frame as communicated by SAP, Partner agrees that SAP shall have no liability for the security or integrity of End User Data to the extent any loss or harm could have been prevented by supporting any upgrade as and when recommended by SAP.
- (m) The SAP Cloud Service ordered by Partner utilized to run the Cloud Application under this Agreement may be used for one (1) or more End User Agreements.
- (n) Partner agrees that its use of the SAP Cloud Service, or the Cloud Application it operates under this Agreement, will not: (a) unreasonably impair, degrade or reduce the performance or security of any SAP software applications, services or related technology; (b) enable the bypassing or circumventing of SAP's license restrictions and/or provide users with access to the SAP Cloud Service to which such users are not licensed; (c) render or provide, without prior written consent from SAP, any information concerning SAP software license terms, the SAP Cloud Service or any other information related to SAP products or services. The Cloud Application will comply with all terms of this Agreement. Partner will not use, and may not authorize any other person or third party to use, any Public Software in connection with the Cloud Application.
- (o) Partner may not use, and may not authorize any other person or third party to use, any Public Software in connection with the SAP Cloud Service in any manner that requires, pursuant to the license applicable to such Public Software, that any SAP software applications or other materials be (i) disclosed or distributed in source code form, (ii) made available free of charge to recipients, or (iii) modifiable without restriction by recipients.
- (p) Partner acknowledges and agrees that SAP or its licensors retain all ownership of and title in and to (including, without limitation, all Intellectual Property Rights) the SAP Materials, including, without limitation, the SAP Cloud Service. Partner does not acquire any ownership rights or title in or to the SAP Materials (including, without limitation, the SAP Cloud Service) and that of SAP's licensors. Partner may not: a) remove or modify any marks or proprietary notices of SAP, b) provide or make the SAP Cloud Service or SAP Materials available to any third party, c) assign this Agreement or give or transfer the SAP Cloud Service, or SAP Materials or an interest in them to another individual or entity, d) decompile, disassemble or reverse engineer (except to the extent permitted by applicable law) the SAP Cloud Service or any SAP Materials, (e) create derivative works of or based on the SAP Cloud Service or SAP Materials, (f) use the Tools to modify existing SAP software or other SAP product functionality or to access the software or other SAP products' source code or metadata.
- (q) If Partner or its End Users are located in mainland China ("China"), Partner and its End Users acknowledge and accept that the SAP Cloud Service is provisioned at the location of SAP's data center outside China, by non-Chinese entities, and it is solely Partner's obligation to ensure use of the SAP Cloud Service and Cloud Application comply with Chinese laws. Notwithstanding anything else in this Agreement, (i) Partner and its End Users are solely responsible for obtaining Internet connection to the SAP Cloud Service from within China and (ii) SAP is not providing any form of telecommunication service under the Agreement (and any representation or warranty to such effect is disclaimed).
- (r) Data Manipulation. Data Manipulation by End Users or Partner may be performed on the SAP HANA Cloud Platform via SQL Access. However, business intelligence or other analytics functionalities, including, without limitation to, data loading, modeling, reporting and distribution, creation and extension of tables, must be performed via the Cloud Application. SQL Access is limited to runtime use with the SAP Cloud Service only.

## 3.2. ADDITIONAL PRODUCT-SPECIFIC USE RIGHTS

### 3.2.1 SAP HANA DB Services

- (a) Use of the SAP HANA Database Service includes a subscription license to SAP HANA and/or SAP ASE for the term of the subscription. Partner is not entitled to receive a physical or downloaded electronic copy of SAP HANA and/or SAP ASE under this subscription license. Partner may not link or combine multiple instances of SAP HANA and/or SAP ASE under separate Agreements.
- (b) Partner acknowledges that SAP may make available a connection between End User or Partner systems and the SAP HANA Database Service in order to upload any data, and as part of such connection, End User or Partner, as the case may be, is required to download a client to its systems. Partner and End Users, as the case may be, shall ensure the client remains secure and shall not use the client for any purpose not expressly permitted in this Agreement. Upon termination of the subscription to the SAP Cloud Service, Partner and End User shall destroy the client and shall have no further right to use the client.
- (c) Monthly data exports from the SAP HANA Database Service are limited to the amount of data storage included in the applicable subscription.
- (d) Other than the Cloud Application, no other software may be uploaded into SAP HANA Database Service or the SAP HANA Cloud Platform unless approved by SAP in writing. SAP reserves the right to exclude any software

from the SAP HANA Database Service to the extent SAP has reason to believe it may harm SAP or any third party or infringe or violate any third party rights. SAP provides no support for Cloud Application under this Agreement, nor shall SAP be responsible for upgrades to the Cloud Application under this Agreement. Partner is responsible for maintaining compatibility between Cloud Application and SAP HANA Database Service upon upgrades of either component.

### 3.2.2 SAP Cloud Identity

The usage metric for measuring SAP Cloud Identity is logon requests. A logon request is a single authentication request managed via SAP Cloud Identity. SAP Cloud Identity counts only one logon request per user per day.

### 3.2.3 SAP HANA Cloud Platform mobile services

- (a) Usage metric for the SAP HANA Cloud Platform mobile services are based on concurrent Mobile Users per month. A Mobile User is an individual who registers for a mobile application in the SAP HANA Cloud Platform mobile services. Mobile Users must be employees of End user or End User's Affiliates, or business partners of End User accessing the End User mobile applications solely in support of End User's internal business operations. Concurrent Mobile Users are the aggregated numbers of end users using the SAP Cloud Service through the respectively licensed Bundled Cloud Service by Partner to End User at any one time.
- (b) Data Privacy and Security – Back up of Partner Data and/or End Users Data and network access to allow Partner Data and/or End User Data transfer are not included in the processing operations of the SAP HANA Cloud Platform mobile service.

### 3.2.4 SAP HANA Cloud Connector

In order to support interaction between an on-premise SAP system along with the SAP Cloud Service, Partner must install the SAP HANA Cloud Connector component on-premise. SAP HANA Cloud Connector is available for download via the SAP HANA Cloud Platform Tooling download site at <https://tools.hana.ondemand.com>. If the SAP HANA Cloud Connector is used to connect to SAP systems additional licenses to such SAP systems must be obtained via a separate contract. If SAP HANA Cloud Connector connects to non-SAP systems additional SAP HANA Cloud Connector licenses must be obtained. The use of the SAP HANA Cloud Connector is limited to use with the SAP Cloud Service and Partner may not use the SAP HANA Cloud Connector for any other purpose. The SAP HANA Cloud Connector is part of the SAP Cloud Service and Partner's use is limited to use by Named Users and only for the term of the subscription to the SAP Cloud Service. The SAP HANA Cloud Connector may not be modified or altered in any way except by SAP. Any such modifications will negate SAP's obligation to provide Support and void SAP's warranty obligations under this Agreement. Partner is solely responsible for the security of the SAP HANA Cloud Connector and is responsible for maintaining adequate security measures, including firewalls, to prevent unauthorized access to the Integration Component. Upon termination or expiration of the subscription to the SAP Cloud Service, Partner's right to use the SAP Cloud Connector shall cease.

## 4. PLATFORM AVAILABILITY

4.1 With respect to the SAP Cloud Service, SAP warrants at least ninety-nine point nine percent (99.9%) System Availability over any calendar month, provided:

- a) The Cloud Application runs with minimum 2 application processes/nodes as described in the "neo deploy" command documentation; and
- b) The Cloud Application has an availability check configured according to the "Availability Checks" documentation.

The documentations can be found at <https://help.hana.ondemand.com/help/frameset.htm>

4.2 Should SAP fail to achieve ninety-nine point nine percent (99.9%) System Availability over a calendar month, Partner shall have the right to receive a credit equal to one percent (1%) of its subscription fees for the SAP Cloud Service (for SAP Cloud Service fees only) for that month, for each one tenth of a percent (0.1%) (or portion thereof) by which SAP fails to achieve such level, up to one hundred percent (100%) of the fees for such month. This is Partner's sole and exclusive remedy for any breach of this service level warranty; provided however, that should SAP fail to achieve ninety-nine point nine percent (99.9%) System Availability in each of two (2) consecutive calendar months, Partner shall have the right to terminate the Order Form for cause, in which case SAP will refund to Partner any prepaid fees for the remainder of its subscription term after the date of termination. Claims under this service level warranty must be made in good faith and by submitting a support case within ten (10) business days after the end of the relevant period. System Availability shall exclude any period of unavailability lasting less than five (5) minutes.

4.3 SAP HANA Cloud Platform Portal.

Notwithstanding anything to the contrary in the Agreement, SAP warrants for the SAP HANA Cloud Platform Portal at least ninety-nine point five percent (99.5%) System Availability over any calendar month. Should SAP fail to achieve ninety-nine point five percent (99.5%) System Availability over a calendar month, Partner shall have the right to receive a credit equal to two percent (2%) of its subscription fees for the Service for that month, for each one percent (1%) (or portion thereof) by which SAP fails to achieve such level, up to one hundred percent (100%) of the fees for such month. This is Partner's sole and exclusive remedy for any breach of this service level warranty; provided however, that should SAP fail to achieve ninety-nine point five percent (99.5%) System Availability in each of two (2) consecutive calendar months, Partner shall have the right to

terminate the Order Form for cause, in which case SAP will refund to Partner any prepaid fees for the remainder of its subscription term after the date of termination. Claims under this service level warranty must be made in good faith and by submitting a support case within ten (10) business days after the end of the relevant period. System Availability shall exclude any period of unavailability lasting less than five (5) minutes.

#### 4.4 SAP HANA Cloud Platform mobile services.

Notwithstanding anything to the contrary in the Agreement, SAP warrants for the SAP HANA Cloud Platform mobile services at least ninety-nine point nine percent (99.9%) System Availability for the Platform over any calendar month. Should SAP fail to achieve ninety-nine point nine percent (99.9%) System Availability over a calendar month, Partner shall have the right to receive a credit equal to two percent (2%) of its subscription fees for the SAP HANA Cloud Platform mobile service for that month, for each one percent (1%) (or portion thereof) by which SAP fails to achieve such level, up to one hundred percent (100%) of the fees for such month. This is Partner's sole and exclusive remedy for any breach of this service level warranty; provided however, that should SAP fail to achieve ninety-nine point nine percent (99.9%) System Availability in each of two (2) consecutive calendar months, Partner shall have the right to terminate the Order Form for cause, in which case SAP will refund to Partner any prepaid fees for the remainder of its subscription term after the date of termination. Claims under this service level warranty must be made in good faith and by submitting a support case within ten (10) business days after the end of the relevant period.

### 5. GENERAL OBLIGATIONS OF AND LIMITATIONS TO PARTNER

5.1 Partner shall reasonably cooperate with SAP to enforce the limitations and requirements imposed according to Sections 2.2 (BCS) to the fullest extent possible.

5.2 To the extent the Contractual Documents grant Partner the right to contract directly with the End User for the license of BCS, Partner shall secure the End User's consent to an End User Agreement with terms not less protective of Licensor than SAP's Cloud GTC and applicable Supplemental Terms and Conditions for SAP Cloud Service current as of the effective date of the license for BCS licensed to each End User ("Minimum Terms"). A copy of which may be found at: <http://global.sap.com/corporate-en/our-company/agreements/index.epx> (please select "Western Europe", "SAP Cloud Agreements", "Cloud General Terms and Conditions (Direct) (EMEA, English)", as well as the respective "Supplemental Terms and Conditions" for the respective SAP Cloud Service, to be included in such End User Agreement.

Where Partner decides to use the SAP's Cloud GTC and Supplement Terms and Conditions for its own purposes, Partner shall replace the references to SAP therein with Partner's name. For clarity, Partner is not required to use SAP's Cloud GTC and/or Supplement Terms and Conditions in verbatim provided that the requirements of this section 5.2 are met. Licensor shall be made a third party beneficiary under the End User Agreement. Partner shall ensure that the terms of the End User Agreement are fully effective and binding as required under applicable laws and regulations in the country, territory or jurisdiction in which Partner is distributing the SAP Cloud Service as part of the BCS, whether directly or indirectly. Partner shall be liable to SAP for any breach of the terms of such End User Agreement to the same extent as Partner would be liable to SAP under this Agreement for such a breach by Partner. Partner shall reasonably cooperate with SAP to enforce the limitations and requirements imposed according to Sections 5.2 to the fullest extent possible.

5.3 Pricing for the SAP Cloud Service must be incorporated into the BCS pricing and may not be itemized separately. Partner will independently establish prices and terms for the BCS, provided such terms include those required by the Agreement.

5.4 Partner may not withhold or reduce applicable fees during the term of the SAP Cloud Service subscription regardless of any termination, non-payment, non-use or other conduct or inaction on the part of the corresponding End User. This shall also apply in case SAP suspends access to the SAP Cloud Service for a particular End User for breach of the Minimum Terms.

5.5 Partner shall not make any representations or warranties regarding the functionality or performance of the SAP Cloud Service other than in accordance with the Agreement.

5.6 Partner is responsible for ensuring that its Cloud Application is capable of automatic restart without manual operator intervention in the event of hardware or system failure occurring within the SAP Cloud Service. This includes ensuring that the Cloud Application connection to on-premise enterprise systems will be automatically restored upon system restart. SAP shall have no liability to Partner for failure of Cloud Application to be built in a manner that it is fail safe and can restore its running state once the Cloud Application is started by the Platform, including failure to achieve any SLA.

6. Intentionally left blank

### 7. SUPPORT

7.1 End User Support by Partner.

Partner shall provide Tier 1 and Tier 2 support to End Users for the SAP 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 Partner 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 Partner is unable to resolve the issue after exhausting its own internal resources, Partner 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 through Partner to End User regarding any updates and assistance in implementing any resolutions received from SAP. Partner will appoint at least two system administrators (“**System Administrators**”) who may contact SAP directly for escalations. In addition, Partner 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. In general, Partner is expected to resolve the majority of the inquiries received by Partner from End Users directly, which may include, but are not limited to, “how to”, feature questions, or “Service not working” issues.

## 7.2 Partner Support.

SAP shall provide support services for the SAP Cloud Service to Partner as described in Exhibit K-2 (OEM Cloud Support). SAP shall be responsible for responding to issues escalated and submitted by Partner that contain the required information as directed by SAP. SAP will respond directly to Partner as outlined in SAP’s then-current support policy for the applicable SAP Cloud Service, which SAP may change in its sole discretion and make available to Partner 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 SAP Cloud Service with any third party service or otherwise contemplated in the Documentation, if the problem cannot be reproduced in the SAP 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.

## 8. MAINTENANCE WINDOWS

### 8.1 SAP HANA Cloud Platform.

SAP can use the maintenance windows for planned downtimes as stated for HANA Cloud Platform on SAP’s public website, to be found at: <http://www.sap.com/corporate-en/about/our-company/policies/cloud/service-level-agreement.html>

### 8.2 SAP HANA Cloud Platform Portal

SAP can use the maintenance windows for planned downtimes as stated for SAP HANA Cloud Portal on SAP’s public website, to be found at: <http://www.sap.com/corporate-en/about/our-company/policies/cloud/service-level-agreement.html>:

### 8.3 SAP HANA Cloud Platform mobile services

SAP can use the following maintenance windows for planned downtimes:

Maintenance Windows	
Regular Maintenance Windows	Bi-weekly, in odd calendar weeks (e.g., calendar week 1, 3, 5, etc.), Thursday morning 7:00 a.m. to 8:00 a.m. Central European Time (CET) for data centers in Europe and 10:00 a.m. to 11:00 a.m. Central European Time (CET) for data centers in America.
Major Upgrades	Up to 4 times per year from Friday 10:00 p.m. to Monday 3:00 a.m. Coordinated Universal Time.(*). SAP will inform Partner in due time in advance (either by email or by any other electronic means).

(*) Coordinated Universal Time	UTC -5 America UTC +2 Europe UTC +8 APA
--------------------------------	---

## 9. TERM AND TERMINATION

9.1 This Agreement, any Order Form and Schedules may be terminated by either party for good cause upon written notice to the other in accordance with the following:

(a) thirty (30) days after a party gives the other party notice of breach of any provision of the Agreement (other than Partner’s breach of its obligations under Sections 2 (Grant of Rights) or 12 (Data Protection), which breach shall give right to immediate termination), Order Form or Schedule, unless the breaching party has cured such breach during such thirty day period;

(b) immediately if Partner does not pay on the due date any amount payable to SAP unless payment is made within thirty (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.

(d) thirty (30) days after SAP gives Partner written notice to terminate, if Partner objects to the use of a Subprocessor by SAP for legitimate reason.

9.2 In the event of expiration or termination of SAP Cloud Service Subscription for any reason other than Partner's material breach and subject to Partner's continuing compliance with the terms and conditions of the Agreement: Respective SAP Cloud Service Subscription shall continue in full force and effect for a maximum of one (1) year after the effective date of expiration or termination to the extent necessary, and inquired by Partner thirty (30) days prior to expiration or termination, to support existing End Users that have executed an End User Agreement for the remainder of their then current SAP Cloud Service Subscription terms as set forth in this Schedule (the "Wind-Down Period"). During the Wind-Down Period, Partner shall remain authorized to continue business for such existing End Users, to be co-terminus with the then-current SAP Cloud Service Subscription term for such existing End Users until expiration of this Schedule. Termination or expiration of SAP Cloud Service Subscription shall not relieve Partner of its outstanding payment obligations existing at the time of such termination or expiration. Any fees previously paid by Partner are non-refundable. Additionally, the parties hereto agree that communications to End Users and any publications/press releases regarding such termination and mentioning of SAP shall be mutually agreed upon, in writing, prior to distribution.

For clarification purposes: In case Partner does not inquire the Wind-Down Period thirty (30) days prior to expiration or termination, the SAP Cloud Service of the respective SAP Cloud Service Subscription will be decommissioned on the effective date of expiration or termination. It will neither be possible to access the respective SAP Cloud Service nor to re-instate the respective SAP Cloud Service, or retrieve data from the respective SAP Cloud Service after the effective date of expiration or termination.

9.3 Notwithstanding SAP's right to terminate as set forth in Article 9.1 above, in the event of (i) any material breach of this Agreement, Schedules 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 SAP Cloud Service may result in harm to the SAP Cloud Service (including the systems used to provide the SAP 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 and/or Partner Data from the SAP Cloud Service, deactivate user name(s), password(s) and/or otherwise suspend access to the SAP Cloud Service for End User and/or Partner.

9.4 End User and/or Partner shall have the ability to access its End User and/or Partner Data at any time during a subscription term as specified under the applicable Schedule. Furthermore, upon reasonable request, End User and/or Partner may export and retrieve its End User and/or Partner Data during a subscription term, which request will be subject to technical limitations caused by factors such as (i) the size of respective instance of the SAP Cloud Service; and (ii) the nature of End User's and/or Partner's request, e.g., the frequency and/or timing of the export and retrieval. End User and/or Partner shall have the ability to export and retrieve its End User and/or Partner 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 and/or Partner Data. Except when such End User and/or Partner Data has been removed in accordance with Section 9.4, or exported by End User and/or Partner, 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 SAP Cloud Service, including, but not limited to, End User and/or Partner Data, unless and to the extent applicable laws and regulations require further retention of such data.

9.5 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.

9.6 After the expiration of the Wind-Down Period, Partner 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. Partner must certify to SAP in writing that it has satisfied its obligations under this Section.

10. Intentionally left blank

11. Intentionally left blank

## **12. DATA PROTECTION**

12.1 Partner agrees to always stay compliant with SAP's most current Data Processing Agreement ("DPA"), a current copy of which as of the date of the SAP Cloud Service Subscription is attached hereto as Annex 1. SAP may, in its sole discretion, update the DPA and/or make the most current version of the DPA available to Partner online through an SAP-designated website ([www.sap.com/company/legal/index.epx](http://www.sap.com/company/legal/index.epx) (please select "Western Europe" >> "Platform Partner Agreements")), and Partner shall use such current version of the DPA for the purposes described herein. For this purpose, Partner hereby shall secure the End User's consent to an End User Agreement with terms not less protective of Licensor than the DPA current as of the effective date of the SAP Cloud Service Subscription. Partner is not authorized to negotiate and/or accept any amendments to the DPA on behalf of SAP or any of its Group Companies.

12.2 Partner agrees to coordinate with the End User in the event SAP amends the DPA Schedule.

12.3 Partner shall enter into appropriate data protection agreements with its End Users as required by applicable data protection laws.

### **13. MISCELLANEOUS**

Infringement Notice. If SAP is notified by third party or an owner of Intellectual Property Rights that the Partner Contents infringe its rights, SAP may investigate the allegation (including by consulting the Partner) and determine in good faith and in its reasonable discretion whether to remove Partner Contents, which it may do after providing Partner with prior notice regarding such removal within a reasonable time in light of the circumstances. Partner shall take down any and all Partner Contents of which Partner becomes aware is infringing promptly or promptly notify SAP to do so. In no event such take down or removal of the Partner Contents give rise to any liability of SAP to Partner or its End Users for a refund, damages or impose any obligation on SAP for continuing services of the SAP Cloud Service.

### **14. WARRANTIES AND DISCLAIMER**

14.1 SAP warrants that the SAP Cloud Service (excluding any third party products, content or services accessed through the SAP Cloud Service) will substantially conform to the specifications stated in the Documentation during the applicable subscription term for such SAP Cloud Service. The foregoing warranty shall not apply: (i) if the SAP Cloud Service is not used in accordance with this Agreement, the Order Form, Schedules 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 SAP Cloud Service; or (iii) to free (no fee) or trial licenses of the SAP Cloud Service.

14.2 Partner 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 Partner complies with Section 14.2 such that existence of non-conformity is validated, SAP will, at its option: (i) repair the non-conforming SAP Cloud Service; or (ii) return an appropriate portion of any payment made by Partner with respect to the affected portion of the applicable SAP Cloud Service. This is Partner's sole and exclusive remedy under this warranty.

14.4 To the maximum extent permitted by applicable law, 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 SAP Cloud Service or any information technology services, software, hardware or other materials provided under this Agreement, or that the operation of any such services, software, hardware or other material will be uninterrupted or error free.

### **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 Partner, End User or any other person or entity with regards to SAP Cloud Service for an amount of damages in excess of the fees paid for the applicable SAP Cloud Service Subscription 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 the amount paid to SAP during the term of this Agreement. Under no circumstances shall SAP, its Group Companies or SAP's licensors be liable in any amount for special, incidental, consequential, or indirect damages, loss of goodwill 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 Partner. The SAP 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 SAP Cloud Service.

15.3 It is expressly understood and agreed that each and every provision of the Agreement which provides for a limitation of liability, disclaimer of warranties or exclusion of damages, is intended by the parties to be severable and independent of any other provision and to be enforced as such.

15.4 Partner 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 Partner inquiries are not intended to provide legal, tax or other expert advice to Partner, or be a substitute for a lawyer, accountant, or other professional. If Partner 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.

15.5 The foregoing limitation of liability does not apply to willful misconduct or fraud, personal injury or death caused by the negligence or any other liability which cannot be excluded or limited by applicable law.

15.6 Claims. Neither party will bring a legal action under this Agreement more than one year after the cause of action arose.



**Exhibit K-2**  
**- ePaaS Licensing of SAP Cloud Service - OEM Cloud Support -**  
**to the Platform Application Development Cooperation Agreement**

This Exhibit K-2 to the Agreement between Partner and SAP stipulates the terms of Embedded Licensing of SAP Cloud Service OEM Cloud Support available to Partner with regards to using SAP Cloud Service as part of a Bundled Cloud Service. Capitalized terms not defined in this Exhibit shall have the meaning ascribed in the Agreement, including the Definitions Schedule, other applicable Schedules, or set forth herein.

This document (“Support Services Document”) describes the support services provided by SAP for SAP Cloud Service.

**1. Applicability**

This Support Services Document governs the provision of support services by SAP to Partner for the SAP Cloud Service.

**2. Support Services**

SAP will offer support for all malfunctions related to the SAP Cloud Service (each an “**Incident**”). Incidents have to be reported by Partner via the help functionality made available by SAP (or any other support channel introduced by SAP). In the event that SAP must access any of Partner’s systems remotely, e.g. via application sharing,

Partner hereby grants to SAP the permission for such remote access. The following Incident priorities shall apply:

<b>Incident Priorities</b>	<b>Definition</b>	<b>Support Availability</b>	<b>Support Language</b>	<b>Initial Response Time</b>
Very High	The problem has very serious consequences for major business transactions and urgent work cannot be performed. The Incident requires immediate attention because the malfunction can cause serious losses.	24 hours x 7 days a week	English	SAP initial response within 4 hours of confirmation.* SAP will attempt to contact partner within the initial response time to clarify business impact and initiate resolution process.
High	A business transaction does not work and necessary tasks cannot be performed. The Incident requires prompt attention because the malfunction can disrupt the entire productive business flow.	Monday to Friday from 9:00 am – 5:00 pm Local Time (as defined below)	English	SAP initial response within 3 days of confirmation.* SAP will attempt to contact partner within the initial response time to clarify business impact and initiate resolution process.
Medium	A business transaction does not work as expected with minor consequences for the productive operation.			Reasonable response time based on the incident (usually within 4 days).* SAP will attempt to contact partner to clarify business impact and evaluate incident.
Low	The malfunction has only few or no effects on business transactions.			Reasonable response time based on the incident.*

\*Incident receipt at SAP will be confirmed via SAP’s incident management system for all online submitted incidents.

Local Time shall mean the time zone in which the Partner Named User with administrative rights submitting the support request is located.

Software Changes

SAP will proactively apply software updates and patches during the defined maintenance windows. In case a patch needs to be applied outside a maintenance window, SAP will notify Partner in advance.

**3. Partner Obligations/Preconditions**

As a precondition to receive the support services as described in Section 2 above, Partner shall fulfill the following obligations:

Key Users

Partner shall identify at least one English-speaking Named User as a “Key User”. The Key User is responsible for managing all business related tasks of the Service related to Partner’s business, such as:

- (i) Support end users and manage their Incidents. This includes searching for known solutions in available documentation and liaising with SAP support in the event of new problems
- (ii) Manage background jobs and the distribution of business tasks across users;
- (iii) Manage and monitor connections to Partner’s third party systems (if available), such as e-mail, fax, printers;
- (iv) Support the potential adaptation of the Service.

Exploration of self-help tools

In case of Incidents, Partner shall make reasonable effort to explore self-help tools to find already documented solutions.

Remote Support

In the event that SAP needs to access any of Partner’s systems remotely, e.g. via application sharing, Partner hereby grants to SAP the permission for such remote access. Further, Partner names a contact person that – if necessary – grants to SAP the required access rights.

**Exhibit K-3**  
**- ePaaS Licensing of SAP Cloud Service - Commercial Terms -**  
**to the Platform Application Development Cooperation Agreement**

## **1. Definitions**

- 1.1 **"BCS Subscription Price"** means the actual subscription price for BCS to End User, including discounts granted by Partner to End User.
- 1.2 **"BCS Subscription Revenue"** means the applicable cloud subscription revenues due for all BCSs delivered by Partner to End User, received and/or payable, in accordance with the generally accepted accounting principles in the country where Partner is located on a consistent basis. Applicable subscription revenues shall include the entire compensation to Partner by End User for providing BCS to End User as a comprehensive cloud offering. Subscription shall include, but is not limited to, compensation for usage rights of Partner's, SAP's, and any third-party intellectual property and all support, service and maintenance services associated with BCS. Applicable subscription revenues shall exclude one-time implementation or other consulting service fees. BCS Subscription Revenue shall exclude any taxes or tax charges of any kind (including but not limited to, income tax, corporation tax, customs duties, tariffs, excise, gross receipts, sales and use and value added tax). BCS Subscription Revenue shall be based on the BCS Subscription Price or, if applicable, on the Fair Value Substitute of BCS, whatever is greater.
- 1.3 **"Fair Value Substitute of BCS"** means a substitute pricing for BCS used for calculation of BCS Subscription Revenue resp. BCS Royalties, which shall reflect the fair value of the offering. Partner can propose a Fair Value Substitute of BCS to SAP at any time or shall provide a Fair Value Substitute of BCS if requested by SAP, when SAP is of the opinion that the planned or actual BCS Subscription Price does not reflect fair value. SAP has the right to reject proposed Fair Value Substitute of BCS as being non-adequate. In case SAP has rejected a Fair Value Substitute of BCS requested from Partner, SAP has the right to assign an independent auditor who verifies whether the suggested Fair Value Substitute of BCS reflects fair value and, if applicable, suggest a new Fair Value Substitute of BCS to Parties. The Parties agree to be bound to such auditing results. Reasonable costs of SAP's audit shall be paid by Partner if the Fair Value Substitute of BCS determined by independent auditor is higher than the Bundled Cloud Subscription Price. Earliest six (6) months after a Fair Value Substitute of BCS has been agreed, both Parties can request a review of the Fair Value Substitute of BCS based upon clear evidence that the fair value of BCS has materially changed. For clarification purposes: Once a Fair Value Substitute of BCS has been agreed, it is also applicable to all subsequent End User licensing of BCS by Partner.
- 1.4 **"Governor Limits"** means the then current maximum amount of SAP Cloud Service Subscription resources provided by SAP to Partner for use of BCS.

## **2. BCS Royalties – SAP Cloud Service Subscription**

- 2.1 As of the effective date of each subscription to SAP Cloud Service for End User licensing of BCS ("SAP Cloud Service Subscription") until termination, Partner shall pay SAP a percentage of the BCS Subscription Revenue ("BCS Royalties"), stipulated by SAP's then current and applicable pricing information on BCS Royalties as referenced in section 4.
- 2.2 Notwithstanding the foregoing, Partner shall pay to SAP fixed BCS Minimum Royalties for each SAP Cloud Service Subscription, stipulated by SAP's then current and applicable pricing information on BCS Minimum Royalties ("BCS Minimum Royalties") as referenced in section 4. Each BCS Minimum Royalties shall be credited towards the BCS Royalties of its SAP Cloud Service Subscription.
- 2.3 The SAP Cloud Service Subscription will continue to remain in effect for successive subscription periods of three (3) months, with an initial subscription period of three (3) months, following the effective date of the SAP Cloud Service Subscription, until Partner terminates the SAP Cloud Service Subscription with thirty (30) days advance notice.

## **3. Revenue Share Reporting & Payments**

- 3.1 At the end of each calendar quarter, SAP will invoice Partner BCS Minimum Royalties in the agreed currency and at the agreed rate under the Agreement on a prorated basis for that quarter
- 3.2 Within twenty (20) days after the close of each calendar quarter, Partner will deliver to SAP a revenue report of BCS Subscription Revenues for the prior calendar quarter. Partner will provide the report in electronic form according to a template provided by SAP. SAP will inform Partner in writing in case of changes of the reporting format. Any changes or corrections to a submitted report can only be made within thirty (30) calendar days after receipt by SAP. SAP will invoice Partner BCS Royalties in the agreed currency under the Agreement according to the final revenue report and section 3.2.
- 3.3 Partner will pay to SAP all invoices due for SAP Cloud Service Subscription even after termination of the Agreement or Wind-Down Period.
- 3.4 Any amounts payable and invoiced by SAP shall be due within thirty (30) days of the invoice date, independent of End User being in default.
- 3.5 SAP will only invoice Partner as described herein if any amounts due exceed an amount of 500 € to avoid invoicing of small amounts. SAP reserves the right to change the threshold to avoid invoicing of small amounts

and to communicate such changes to Partner. Notwithstanding the foregoing, SAP will always invoice all due fees before the end of each calendar year.

- 3.6 Where SAP and Partner have agreed that SAP will invoice Partner in EURO under the Agreement, the EURO/local currency exchange rate shall be based on the official fixing of the European Central Bank on the last business day of the month immediately preceding the month in which SAP invoices Partner. Where SAP and Partner have agreed that SAP will invoice Partner in USD under the Agreement, the USD/local currency exchange rate shall be based on the official fixing of the Federal Reserve System of the United States of America on the last business day of the month immediately preceding the month in which SAP invoices Partner.
- 3.7 SAP reserves the right to audit Partner's internal records with regards to Bundled Cloud Subscription Revenues in order to verify the consistency between Partner's internal records and reports created by Partner and provided to SAP in accordance with Section 3. The audit right may be executed by SAP or a mutually agreed independent auditor and may be exercised one (1) time in any twelve (12) month period provided that the auditing Party signs customary assurances of confidentiality and the audit is performed in such a manner that it will not disrupt Partner's business. Partner is only required to disclose information that consists of business records reflecting amounts due to SAP or other information proving compliance with the commercial terms under the Agreement. SAP will be responsible for the costs of any audit.
- 3.8 If the audit discloses an underpayment, then Partner will promptly, but no later than within one (1) calendar month, correct this underpayment by paying to SAP the amount of the underpayment. If the underpayment is greater than ten percent (10%) of the total amount payable during the period under audit, then Partner will, in addition to paying the amount of the underpayment, reimburse SAP for the reasonable costs of the audit. In case an audit discloses discrepancies between actual BCS Subscription Revenues and the final amounts reported to SAP in two (2) or more revenue reports, SAP may terminate the Agreement for breach in accordance with the terms of the Agreement.
- 3.9 All payments hereunder are non-refundable. Partner 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 SAP Cloud Service. Fees not paid when due may result in suspension of Partner and its End Users' ability to access the SAP Cloud Service until payment is made.

#### **4. Pricing sheet information on BCS Royalties**

- 4.1 The current percentage of the BCS Royalties can be found in the pricing sheet information within the "Region-Specific Program Information" ("RSPI") applicable to SAP PartnerEdge Silver and Gold Partners which are published on SAP's partner-dedicated website at [www.sappartneredge.com](http://www.sappartneredge.com).
- 4.2 The current BCS Minimum Royalties can be found in the pricing sheet information within the RSPI according to the respective BCS category.
- 4.3 BCS Minimum Royalties per month permanently increase as outlined in the pricing sheet information within the RSPI in case used for more than one (1) End User Agreement per SAP Cloud Service Subscription ("Multi-Tenancy").
- 4.4 SAP reserves the right to verify that the Cloud Application of a Bundled Cloud Service meets the technical requirements to be operated in a Multi-Tenancy mode as described in the Multi-Tenancy verification guidelines at <https://www.sapadpc.com>, and refuse Multi-Tenancy operation of Bundled Cloud Service in case it does not meet such requirements. Partner must provide all information reasonably requested by SAP concerning the Cloud Application of such Bundled Cloud Service and its technical Multi-Tenancy usage scenario. The verification service offered by SAP may be subject to a separate agreement and incur additional fees.
- 4.5 SAP monitors the consumption of SAP Cloud Service Subscription resources caused by BCS. SAP reserves the right to permanently increase the Governor Limits and corresponding BCS Minimum Royalties in case of excess resource consumption of the SAP Cloud Service Subscription. Governor Limits and BCS Minimum Royalties will be increased in increments, or multiples thereof, as outlined in the pricing sheet information within the RSPI, to the degree necessary to cover the detected excess resource consumption. Such permanent increase of Governor Limits and BCS Minimum Royalties takes effect no earlier than at the beginning of the calendar quarter, in which the excess resource consumption of the SAP Cloud Service Subscription has been detected and communicated to Partner by SAP. Partner agrees to pay all requisite fees in accordance with the terms of this Agreement from the effective date SAP has determined and communicated to Partner about the increase of BCS Minimum Royalties.
- 4.6 Notwithstanding the foregoing, Partner may request a permanent increase of Governor Limits, subject to the pricing sheet information within the RSPI and in accordance with the terms of this Agreement. Such permanent increase of Governor Limits and the respective BCS Minimum Royalties can only take effect at the beginning of a calendar quarter.
- 4.7 Once per year, Partner may request and SAP may choose to accept to reduce permanent increases of BCS Minimum Royalties, if (i) number of End User Agreements reduces to one (1) End User Agreement per SAP Cloud Service Subscription or if (ii) the increase of Governor Limits is no longer required. Reductions of Governor Limits and BCS Minimum Royalties will be effective at the beginning of the calendar quarter following the decision on such reduction. SAP reserves the right to incur an additional fee for executing such a reduction of the permanent increases of BCS Minimum Royalties as outlined in the pricing sheet in the then current RSPI.

#### **5. Change terms for ePaaS licensing of SAP Cloud Service**

SAP reserves the right to change, add, or remove Schedules and/or its terms, or fees, or elements of the ePaaS licensing of SAP Cloud Service offering stipulated in the Agreement. SAP communicates such changes to Partner with at least ninety (90) days prior notice, unless a change does not materially diminish SAP's offering to Partner hereunder. Such changes are not effective retroactively and only apply as of the effective date which SAP specifies in the notice. Partner acknowledges its agreement to have these changes apply by either (i) requesting the change if such change request is made available by SAP in its sole discretion (ii) placing new orders or registrations, or (iii) failing to request within the ninety (90) days' notice period that the change effective date shall be deferred until the start of the new renewal period. Renewal of this Agreement shall be subject to SAP's then applicable and communicated terms and fees in effect at such time. Upon renewal, each Party may terminate the Agreement by giving the other Party three (3) months prior written notice to the end of the Initial Term or any Renewal Term.

**ANNEX 1**  
**Data Processing Agreement**

**Data Processing Agreement (“DPA”)**

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

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

and:

**Partner Name:** \_\_\_\_\_

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

SAP and Partner are herein individually referred to as a “Party” and jointly referred to as the “Parties”.

**PREAMBLE:**

WHEREAS Partner subscribes to ePaaS licensing of SAP Cloud Service under the Agreement whereby SAP grants to Partner the right to use the SAP Cloud Service to operate the Cloud Application only for use in conjunction with, and for purposes of, Cloud Application to End Users, whereby End User for the purpose of this Annex 1 shall only mean a Legal Entity to which Partner provides access to BCSs pursuant to the terms of the Agreement; and

WHEREAS SAP will provide certain hosting and/or maintenance and support services for Partner and End Users on behalf of Partner in conjunction with the SAP Cloud Service of the BCS. These hosting and/or maintenance and support services may include the processing of and/or access to personal data controlled by Partner and End Users as defined in Directive 95/46 EC; and

WHEREAS any such processing of personal data requires the prior entry into a data processing agreement between all parties of the data processing chain: i.e. (i) a data processing agreement between End User as the data controller and Partner as End User’s data processor and (ii) another data processing agreement (i.e. this Data Processing Agreement) between Partner as data processor and SAP as Partner’s data sub-processor is required.

WHEREAS Partner understands and acknowledges that since SAP’s processing services of personal data represent the vast majority of the processing of personal data in connection with the SAP Cloud Service that SAP’s terms for the processing of personal data shall prevail and that Partner will mirror the terms of this Data Processing Agreement to Partner’s own data processing agreements with any End Users.

NOW, THEREFORE, the Parties agree as follows:

SAP and Partner agree that this Data Processing Agreement stipulates the rights and obligations of Partner and SAP in connection with personal data processed by SAP on behalf of Partner and/or End Users solely for the SAP Cloud Service. References to “**Affiliates**” 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 Annex 1 including its appendices shall become an integral part of the ePaaS licensing of SAP Cloud Service Schedule. Any capitalized terms referenced but not defined herein shall have the meaning given to them in the Agreement. This Annex 1 in conjunction with its appendices stipulates:

- a) the rights and obligations of Partner and SAP in connection with personal data that SAP and its authorized Subprocessors process on behalf of Partner and/or End Users pursuant to the ePaaS licensing of SAP Cloud Service Schedule; and
- b) the applicable technical and organizational measures SAP implements and maintains to protect Partner’s and/or End Users’ personal data.

**1. Definitions**

“**Data exporter**” as defined in the Standard Contractual Clauses shall mean Partner and/or End Users.

“**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 6 below.

**2. Data Processing Purposes**

2.1 Partner, on behalf of itself or as directed by End Users as the respective data controller(s), shall determine the purposes of collecting, processing, and otherwise using personal data stored in the SAP Cloud Service. Appendix 1 of the Standard Contractual Clauses attached hereto shall apply to such data processing. Before Partner or any End User will store any special categories of personal data (e.g. health data, political beliefs, trade union membership) in the SAP Cloud Service, Partner will inform SAP. Partner and SAP will then discuss in good faith whether and if so under which conditions storage of special categories of personal data in the SAP Cloud Service is possible.

2.2 The purposes for processing personal data stored in the SAP Cloud Service or otherwise provided to SAP and its Subprocessors under the relevant Agreements are limited to:

- a) Setting up, operating, monitoring and providing the SAP Cloud 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 ePaaS licensing of SAP Cloud Service Schedule;
- b) Providing technical support as a main obligation of SAP under the ePaaS licensing of SAP Cloud Service Schedule;

- 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 Partner and/or End Users that SAP hosts in an EU based data center; or (b) hosts personal data from Partner and/or End Users who are incorporated in a member state of the EU/EEA or Switzerland in a data center outside the EU. In case End Users will be the data exporters, Partner will procure that the End Users grant Partner a power of attorney to enter into the Standard Contractual Clauses with the Non EU Entity on behalf of the relevant End Users. 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. Partner acknowledges (i) it has had the opportunity to review the Standard Contractual Clauses or to obtain a full copy from SAP and (ii) it will provide a copy of the Standard Contractual Clauses to End Users.

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 Partner with thirty (30) days prior written notice (email permitted) thereof. Partner will then flow down the respective changes to its End Users.

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 Annex 1.

### **4. Partner's Obligations**

4.1 As between SAP and Partner, Partner shall be solely responsible for the permissibility of the processing of personal data as well as for safeguarding the rights of the data subjects.

4.2 Partner shall inform SAP without delay, if Partner or an End User detects errors or irregularities when examining the results of the processing of personal data.

4.3 Partner will enter into data processing agreements with End Users where legally required which mirror the terms of this Data Processing Agreement.

### **5. SAP Obligations**

5.1 SAP shall process personal data and other operating data of Partner and/or End Users as provided to SAP by Partner only in accordance with Partner's instructions and/or the instructions of End Users as forwarded to SAP by Partner. Where Partner's and End Users' instructions contradict and relate to End Users' personal data the instructions of End Users shall prevail. These instructions may include (without limitation) the correction, erasure and/or the blocking of personal data if and to the extent the functionality of the SAP Cloud Service does not allow the Partner and/or End User to do so. SAP shall notify Partner if SAP considers an instruction given by Partner on behalf of itself or on behalf of End Users to be in violation of data protection laws. SAP shall not be obligated to perform a comprehensive legal examination.

5.2 For processing personal data, SAP shall only use personnel who have committed themselves to observe data secrecy and (to the extent applicable) 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 personal data are regularly trained on data security and data protection.

5.3 SAP shall implement all technical and organizational measures to comply with requirements pursuant to applicable data protection laws as further set out in this section: SAP undertakes to Partner that it has taken and will, on a continuing basis, take appropriate technical and organizational measures to keep Partner's and End Users' personal 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 of this Annex 1:

- 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 SAP Cloud Service by its personnel, as required to operate, maintain, support or secure the SAP Cloud Service.
- d) Transmission control: SAP shall ensure Partner's data transmission in encrypted form or by a secure alternative procedure. Transmissions must be logged and guidelines for Partner's 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 Partner's and End Users' data to the greatest extent supported by the SAP Cloud Service.
- f) Job control: SAP shall define in writing and establish control mechanisms to ensure that Partner's and End Users' data is processed strictly in accordance with the instructions of Partner or End Users as provided to SAP by Partner and as contemplated in the ePaaS licensing of SAP Cloud Service Schedule.
- g) Availability control. SAP shall run a state of the art backup system and define a restore operation procedure to protect Partner's and End Users' data from accidental destruction or loss.
- h) Data separation: SAP shall ensure by technical means and defined organizational procedures that Partner's and End Users' data collected for different purposes (e.g., different End Users) can be processed separately. Technical means can be separated computer systems or demonstrably logical separation in a multi-tenant architecture. Access by another partner or its end users to the data of Partner or End Users must be prevented.

SAP provides the SAP Cloud Service to all customers (including Partner and its End Users) 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 SAP Cloud Service. Furthermore, Partner 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 Partner by email or publication on a website easily accessible by Partner. Partner will then flow down the respective notifications and changes to End Users.

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

5.5 SAP shall promptly inform Partner in the event of serious disruptions of the operating process, suspected data protection violations or other irregularities in connection with the processing of Partner's or End Users' personal data.

5.6 At Partner's written request and at Partner's expense, SAP shall reasonably support Partner 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 Partner about inspections and measures of a supervisory or other competent authority relevant for Partner's or End Users' personal data.

## **6. Subprocessors**

Partner 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 ePaaS licensing of SAP Cloud Service Schedule 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 obligations as data (sub-) processor vis-à-vis Partner as set out in this Annex 1 and obligate Subprocessors to obey all relevant data protection rules. SAP will inform Partner upon its request by email or through a web site accessible to Partner 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 Partner by email or otherwise in advance of any changes to the list of Subprocessors. If Partner has a legitimate reason to object to SAP's use of a Subprocessor Partner shall notify SAP thereof in writing within sixty (60) days after receipt of SAP's notice. If Partner does not object during such time period the new Subprocessor(s) shall be deemed accepted. If Partner objects to the use of the Subprocessor concerned SAP shall have the right to either provide the SAP Cloud Service without such Subprocessor or to terminate the subscription to embedded licensing for SAP 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 hereunder. 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.

## **7. Monitoring Rights of Partner**

7.1 During the term of the subscription to ePaaS licensing of SAP Cloud Service, SAP shall maintain, at its own expense, applicable certifications or audit reports. Unless provided otherwise in a supplement, SAP engages a nationally recognized independent third party auditor to review the measures in place in protection of the SAP Cloud Service(s). Certifications may be based on ISO 27001 or other standards (scope as defined in certificate). For certain SAP Cloud Service, SAP performs regular audits (at least annually) via certified auditors to provide a valid SOC 1 Type 2 (SSAE 16 or ISAE 3402) and/or SOC 2 Type 2 report. Audit reports are available through the third party auditor or SAP, as applicable. Upon Partner's request, SAP shall inform the Partner about the applicable certifications and audit standards available for the Service concerned.

7.2 If SAP fails to perform its audit obligations hereunder, and has not provided sufficient evidence of this compliance after Partner's written request, Partner and End Users (or an independent third party auditor on their 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 sixty (60) days) and under reasonable time, place and manner conditions.

7.3 Furthermore, Partner and End Users may also audit SAP's control environment and security practices relevant to personal data processed hereunder if they have reasonable grounds to believe that SAP is processing their personal data not duly. In this case, the prior notice of sixty (60) days is not required.

7.4 SAP shall reasonably support Partner and End Users throughout these verification processes and provide Partner and End Users with the required information. Partner shall bear any costs (including SAP's internal resource based on then-current daily professional service rates per SAP's price list) in cases other than where Partner and/or End Users have reasonable grounds to believe that SAP is processing their personal data not duly.

## **8. General Provisions.**

8.1 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 Partner at the address first set forth above.

8.2 Any delay or nonperformance of any provision of this Annex 1 caused by conditions beyond the reasonable control of SAP shall not constitute a breach of this Annex 1, 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.

Accepted by:

SAP:

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

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

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

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

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

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

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

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

Partner: [ \_\_\_\_\_ ]

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

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

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

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



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

### **Data exporter**

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

The data exporter (i.e. Partner) uses certain SAP Cloud Service to operate the Cloud Application only for use in conjunction with, and for purposes of provision and support of Cloud Application which allows End Users to enter, amend, use, delete or otherwise process End User data in SAP's systems as contemplated under the ePaaS licensing of SAP Cloud Service Schedule.

### **Data importer**

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

SAP and its Subprocessors provide certain SAP Cloud Service to Partner which include the hosting of the Cloud Application and the provision of technical support to Partner as contemplated under the ePaaS licensing of SAP Cloud Service Schedule.

### **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, customers or other individuals whose personal data is stored in the SAP Cloud Service.

### **Categories of data**

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

Partner's End Users determine the categories of personal data per BCS subscribed. End Users' data fields can be configured as part of using the BCS or as otherwise permitted in the BCS. 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 End Users' users enter into the BCS.

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

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

As agreed between SAP and Partner in accordance with Section 2.1 above.

### **Processing operations**

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

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

## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES AND ANNEX 1

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

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: 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 and own 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 personal data of Partner and End Users shall include the following measures:
  - monitoring capability in respect of individuals who delete, add or modify the exported 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 Partner 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 personal 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;
  - electronic recording of entries (as further specified by SAP).

#### **6. Job control**

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

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

- clearly defined responsibilities;
- criteria for selection of SAP, as determined and communicated by Partner;
- 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;
- uninterruptible power supply (UPS);
- separate storage;
- antivirus / firewall.

## 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:

- SAP uses the technical capabilities of the deployed software (for example: multi-tenancy or separate system landscapes) to achieve data separation between personal data from one and any other partner.
- SAP maintains dedicated instances for each partner.
- Partners (including their affiliates) have access only to own partner 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 Partner 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 Partner or End User information is classified lower than "confidential".
- Access to Partner and End User 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 Partner and End User 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, Partner and End Users have control over their remote support connections. SAP employees cannot access a Partner or End User system without the knowledge or full active support of the Partner and End Users.
- All SAP employees and contractual partners are contractual bound to respect the confidentiality of all sensitive information including information about the trade secrets of Partner and End User.
- During the support process, the personal data of different partners and end users 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 SAP Cloud Service.