

**Order Form
for SAP Cloud Services
SAP Reference No. 0220558288**

Between **SuccessFactors, Inc.**
1 Tower Place, Suite 1100,
South San Francisco, CA 94080
("SAP")

And The School Board of Broward County, Florida
7720 W Oakland Park Blvd / SUNRISE FL 33351-6704 Floor
("Customer")

1. ORDER FORM AND TABLE OF AGREEMENT

This Order Form as issued by SAP is an offer by SAP. When signed and returned to SAP by Customer on or prior to the offer expiration date, it becomes a binding agreement for the SAP Cloud Service(s) and Consulting Services (if applicable) listed in this Order Form and is effective on the date signed by Customer.

Offer Expiration Date: 07/26/2016

This Order Form is governed by and incorporates the following documents in effect as of the effective date. All documents are listed in order of precedence, and collectively referred to as the **"Agreement"**:

Order Form	
Schedule A of this Order Form: a) Cloud Service Supplemental Terms and Conditions may also be referenced as the "SAP SuccessFactors HCM Suite Supplemental terms and conditions" (" Supplement ")	a) http://go.sap.com/about/agreements/cloud-services-english-supplement.html (Schedule A)
Schedule B of this Order Form: Support Policy for SAP Cloud Services	http://go.sap.com/about/agreements/cloud-services.html?search=Support%20Cloud%20Edition (Schedule B)
Schedule C of this Order Form: Service Level Agreement for SAP Cloud Services ("SLA")	http://go.sap.com/about/agreements/cloud-services.html?search=Service%20Level%20Agreement (Schedule C)
Schedule D of this Order Form: Data Processing Agreement for SAP Cloud Services Schedule D will serve as a commissioned written data processing agreement.	http://go.sap.com/about/agreements/cloud-services.html?search=data%20processing (Schedule D)
Schedule E of this Order Form: General Terms and Conditions for SAP Cloud Services ("GTC")	http://go.sap.com/docs/download/agreements/general-terms-and-conditions/cls/general-terms-and-conditions-for-sap-cloud-services-direct-us-english-v4-2016.pdf (Schedule E)

Customer has had the opportunity to review the GTC and the incorporated documents prior to executing this Order Form. SAP recommends that Customer prints copies of these documents for Customer's records. All defined terms in the GTC used in this Order Form have the meaning stated in the GTC. All references in the Supplements to "Service" mean "Cloud Service", and to "Named Users" mean "Authorized Users."

2. CLOUD SERVICE

2.1 Cloud Service Order.

The table shows the purchased Cloud Service, Usage Metrics and volume, Initial Subscription Term and fees.

Period 1 From 06/29/2016 To 06/28/2017

SAP Cloud Service	Usage metric	Usage Metric Limitation	Product Start Date	Product End Date	Total fee in USD
SAP SFSF Succession & Development	Users	5,000	06/29/2016	06/28/2017	43,210.00

Total net fee (*)	43,210.00
-------------------	-----------

Period 2 From 06/29/2017 To 06/28/2018

SAP Cloud Service	Usage metric	Usage Metric Limitation	Product Start Date	Product End Date	Total fee in USD
SAP SFSF Succession & Development	Users	5,000	06/29/2017	06/28/2018	43,210.00

Total net fee (*)	43,210.00
-------------------	-----------

Period 3 From 06/29/2018 To 06/28/2019

SAP Cloud Service	Usage metric	Usage Metric Limitation	Product Start Date	Product End Date	Total fee in USD
SAP SFSF Succession & Development	Users	5,000	06/29/2018	06/28/2019	43,210.00

Total net fee (*)	43,210.00
-------------------	-----------

2.2 Subscription Term

- (a) Customer's Initial Subscription Term will begin on the start date and will be effective until the end date, unless Customer is otherwise notified by SAP.
- (b) Unless terminated earlier, pursuant to Section 7 of this Agreement, the term of this Agreement shall be for a period of three (3) years from the date of award, with the option of 2 (two) 1 (one) year renewals upon mutual written agreement between Customer and SAP.

2.3 Excess Use.

Customer's use of the Cloud Service is subject to the Agreement, including the Usage Metrics and their volume stated in Section 2. Any use of the Cloud Service that exceeds this scope will be subject to additional fees. Fees accrue from the date the excess use began. Customer will execute an additional Order Form to document subscriptions for additional Usage Metrics and their volume. SAP may invoice and Customer will pay for excess use based on applicable pricing in the Order Form or Supplement.

2.4 Security Breach.

In the event SAP discovers or is notified of a material security breach of the Cloud Service, which impacts Customer, whether such breach is internal or external, that results in the public exposure of, and damage to, Customer or any of the Customer Data, SAP shall (i) notify the appropriate Customer personnel; (ii) investigate the breach or potential breach; (iii) provide Customer with the results of the investigation; and (iv) if requested by Customer at any time before, during or after the investigation, reasonably cooperate with Customer's investigation of such breach or potential breach.

3. RESERVED.

4. PAYMENT AND INVOICES

4.1 Fees and Invoicing.

Unless the Supplement states otherwise, fees for the Cloud Service(s) will be invoiced by SAP and paid by Customer annually in advance. Fees for the Consulting Services will be invoiced by SAP and paid by Customer as stated in Section 3 unless otherwise stated in the applicable scope document. SAP may provide invoices to an email address provided by Customer. Fees for non-recurring services will be invoiced by SAP on a one-time basis and paid by Customer upon commencement of the Subscription Term. Except for fee increases applied under Sections 2.3 and 4.2, Cloud Service(s) fees for renewal terms will be equal to the fees for the immediately preceding term for the same Cloud Service, Usage Metrics and volume.

4.2 Fee Increases.

At the beginning of each renewal term, SAP may increase fees to reflect annual increases in consumer prices or costs. This increase will not exceed the greater of the percentage stated in the most recent consumer price index selected by SAP or 3.3% per annum. The increase is applied on a cumulative, year-over-year basis beginning on either the start of the preceding term or date of last increase, whichever is later. Not raising fees is not a waiver of SAP's right to do so. SAP may increase fees if Customer elects to reduce the Cloud Service, Usage Metrics or volume for any renewal term.

4.3 Payment.

Customer will pay to SAP all fees due within thirty days of date of invoice. Unpaid fees that are not subject to a good faith dispute regarding such payment of which SAP has been made aware in a timely manner will accrue interest at the maximum legal rate. Customer purchase orders are for administrative convenience and not a condition of payment. Payment is not dependent upon completion of any implementation or other services. Any dispute of fees due hereunder must (a) be made in good faith within fifteen (15) days of invoice date, and (b) must involve an invoicing error of the amount due or the due date.

5. AUTHORIZED ADMINISTRATORS

Customer contacts for order confirmation and system notices are:

Order confirmation recipient name:
Order confirmation recipient e-mail:
System provisioning notification recipient name:
System provisioning notification recipient e-mail:

Ed Hinline
ed.hinline@browardschools.com
Ed Hinline
ed.hinline@browardschools.com

6. CUSTOMER LOCATION

Customer has provided the following primary access location:

The School Board of Broward County
7720 W Oakland Park Blvd / SUNRISE FL 33351-6704

This is the primary (but not the only) location from which Customer will access the Cloud Service. If Customer does not provide a primary access location, SAP will incorporate a default primary access location to Customer's sold-to address. The primary access location is used by SAP for the determination of any applicable taxes.

7. NON-APPROPRIATION TERMINATION

Any payment obligation of the Customer created by the Agreement is conditioned upon the availability and appropriation of funds, subject to this Section 7. If funds are not appropriated to support continuation of performance in a subsequent fiscal year period, Customer shall have the right to terminate the Agreement at the end of the then current pre-paid annual subscription period with written notice to SAP at least thirty (30) days prior to the start of the next annual subscription period (a "Non-Appropriation Termination"), provided, however, Customer shall not be entitled to any refund of any prepaid fees and shall be responsible for payment of amounts incurred up to the date of such termination.

Accepted By:

**The School Board of Broward County,
Florida (Customer)**

Name: Dr. Rosalind Osgood

Title: Chair

Date:

Accepted By:

**SuccessFactors, Inc.
(SAP)**

Name:

Title:

Date:

**MARK BUCKLEY
DIRECTOR-CONTRACTS**

6/15/2016

Name: Robert W. Runcie

Title: Superintendent of Schools

Date:

Approved as to Form and Legal Content:

Office of the General Counsel

Digitally signed by Kathelyn Jacques-Adams
DN: cn=Kathelyn Jacques-Adams, o=The School District of
Broward County, Florida, ou=The Office of the General
Counsel, email=kathelyn.jacques-
adams@browardschools.com, c=US
Date: 2016.06.20 15:17:23 -04'00'

Title:

Date:

SAP

**Order Form for SAP Cloud Services (Direct) enUS 0750.v.4-2016
SAP OPP 302182043 / QUOTE 0220558288 / CASE 3060552638**

**Page 5 of 5
(4-2016)**

**SAP SuccessFactors HCM Suite
Supplemental Terms and Conditions**

These supplemental terms and conditions ("the Supplement") are part of an agreement for certain SAP cloud services ("Agreement") between SAP and Customer and apply solely to SAP SuccessFactors HCM Suite (the "Cloud Service") and not any other SAP product or service.

1. CLOUD SERVICE

1.1 SAP may use Customer Data for developing and distributing benchmarks and similar reports and databases therefrom so long as SAP (a) first removes all references to Customer and any personal information of an Authorized User included in the Customer Data; (b) presents such Customer Data in the form of aggregate benchmarks; and (c) generates and publishes benchmarks only when such benchmarks include data from at least seven (7) other organizations.

1.2 Packages ("Packages") consist of several SAP products ("Products") and some Products consist of several SAP modules. Packaged pricing for the Cloud Service, if applicable, will not be disaggregated and Customer shall not be entitled to credits, swaps or other concessions associated therewith. Packages and Products do not include any new products or modules that may be released after the Effective Date of the applicable Order Form. Package and Product descriptions are set forth in Appendix 1.

1.3 Not all content is available in each language but that language packs may only provide translations for the text strings used in the software system interface, not the content such as goals wizards texts and the like.

An Enterprise Language Pack ("ELP"), which is included with Customer's subscription for so long as Customer continues to subscribe to the Cloud Service, includes language packs that SAP presently and in the future makes generally available thereunder. Access to and delivery of any future language packs will occur only when such language packs are made generally available to all customers. Implementation service fees set forth in an Order Form, if any, are only for those language packs Customer has initially selected for implementation. Implementation of any additional language packs will result in additional service fees, which fees will be documented in an additional Order Form or addendum. For clarity, ELP is not included with subscriptions to SAP Jam, Employee Central Payroll, Perform & Reward for Small Business, SuccessFactors Employee Central Service Center or SAP HANA Cloud Platform, extension package for SuccessFactors.

1.4 If Customer subscribes to Lominger, the following shall apply:

Lominger Limited, Inc. ("Lominger") content provided under an Order Form is a third party product that will be subject to the separate terms and conditions set forth below. SAP disclaims any responsibility for such third party product. Lominger owns all rights in the titles and text, including all updates, revisions, and upgrades thereto, of the Lominger products known as (a) The Leadership Architect® Sort Cards 04.1b-INTL English; (b) The Leadership Architect® Competency Aspects v02.1a – English; (c) FYI For Your Improvement™ – 4th Edition – English; and (d) 10 Universal Performance Dimensions Titles and Definitions (collectively the "Lominger Provided Content"). Such Lominger Provided Content is subject to the following conditions:

Customer's use of the Lominger Provided Content shall not extend outside of the Cloud Service other than in material specifically used in the context of training around the Cloud Service. In the event Customer wishes to use the Lominger Provided Content for any other purpose, in any form, or create any derivatives thereof, Customer shall enter into a separate license agreement with Lominger for such extended use of the Lominger Provided Content.

The Lominger Provided Content contains the proprietary works of Lominger and is deemed Confidential Information. Customer will not allow the Lominger Provided Content to be disclosed, copied by, or otherwise transferred to any person or entity outside of Customer. The Lominger Provided Content is for Customer's use in certain SAP modules, as made generally available by Lominger, may only be used within the Cloud Service and may not be edited.

1.5 The Cloud Service may be accessed by Authorized Users through a mobile application obtained by Authorized Users via third-party websites (e.g.: Android or Apple app store). The use of such mobile

applications is governed by the terms and conditions presented to the Authorized User upon download/access to the mobile application and not by the terms of the Agreement. The third party that operates the website through which the mobile application is distributed may stop distributing the mobile application at any time, and SAP is not responsible for the unavailability of the mobile application due to the actions of the third party distributor.

2. FEES

2.1 Authorized User Usage Metric. "Authorized Users" shall, in addition to that set forth in the Agreement, also include Customer's and its Affiliates' employees and Business Partners whose information is stored on the Cloud Service and who have an active profile/status against which the Cloud Service is processing transactions. Pricing for the SAP SuccessFactors Advanced Learning Package, SAP SuccessFactors Perform & Reward Package, SAP SuccessFactors Performance & Goals Product, SAP SuccessFactors Compensation Product, SAP SuccessFactors Succession & Career Development Product, SAP SuccessFactors Learning Product, SAP SuccessFactors Validated Learning Product, SAP SuccessFactors Employee Central Product, Employee Central Payroll Product, SAP Jam Product and Perform & Reward for Small Business, is based on Authorized Users.

2.2 Employee Usage Metric. "Employees" means the number of Customer's (and its participating Affiliates') total employee population. Pricing for the SAP SuccessFactors Talent Management Package, SAP SuccessFactors Enterprise Package, SAP SuccessFactors Onboarding, SAP SuccessFactors Recruiting Execution Product, SAP SuccessFactors Recruiting Marketing Product, SAP SuccessFactors Recruiting Management Product, SAP SuccessFactors Workforce Analytics & Planning Product, SAP SuccessFactors Workforce Planning Product, SAP SuccessFactors Workforce Analytics Product, SuccessFactors Employee Central Service Center and SAP HANA Cloud Platform, extension package for SuccessFactors, is based on Employees.

2.3 For purposes of calculating pricing, Authorized Users or Employees, as applicable, shall exclude (a) individuals who do not have an active profile/status on the Cloud Service; (b) external candidates using the Recruiting Management Cloud Service or Recruiting Marketing Cloud Service to respond to employment opportunities; and (c) external raters using the 360 Degree Reviews Cloud Service to perform reviews.

3. SERVICE SPECIFIC ADDITIONAL TERMS. The terms below apply solely to the identified Cloud Services and prevail over any conflicting terms in the Agreement.

3.1 Jam Cloud Service

(a) **"User Content"** means information that is uploaded to the Jam Cloud Service by Authorized Users. User Content shall be considered Customer Data.

(b) **User Content Disclaimer.** If SAP is notified by an Authorized User or an owner of User Content that the User Content allegedly infringes its rights, SAP may investigate the allegation (including by consulting with Customer) and determine in good faith and in its reasonable discretion whether to remove the User Content, which it may do after providing Customer 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 Authorized Users or Customer and its Authorized Users. Customer 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.

(c) **Storage.** The following Gigabyte (GB) storage limits apply to the Jam Cloud Service:

SAP Jam, basic edition: 2 GB per instance

SAP Jam, advanced edition: 100 GB per instance

SAP Jam, advanced plus edition: 200 GB per instance

SAP Jam, enterprise edition: 1000 GB per instance

If subscribed to, "Jam Collaboration, data storage add-on additional storage" entitles Customer to the specified additional units of storage set forth in the applicable Order Form. One unit of storage equals five hundred (500) GBs.

3.2 Recruiting Marketing (RM) Cloud Service

(a) Definitions.

(i) **"Candidate Information"** means personal data and personally identifiable information associated with potential candidates, including, but not limited to, name and email address. Candidate Information shall be considered Customer Data.

(ii) **"Customer Content"** means graphics, branding and job requisition content made available by Customer to SAP. Customer Content shall be considered Customer Data.

(iii) **"Recruiting Dashboard"** means the on-line tool included with the RM Cloud Service that provides Customer with reports and metrics.

(b) Customer Content. In connection with the RM Cloud Service, Customer will make Customer Content available to SAP. The RM Cloud Service requires access to Customer Content from Customer's career site and/or Applicant Tracking System ("ATS"), therefore Customer is responsible for ensuring that SAP has daily access to Customer Content, and Customer will provide SAP with at least two weeks' written notice of any modifications to Customer's career site or ATS.

As applicable, SAP will create a Customer website ("Customer Website") with Customer Content within the standard RM Cloud Service layout, subject to an implementation requirements document to be mutually agreed to prior to the start of the implementation.

(c) Candidate Information Restrictions and Authorized Use. Customer shall use, display and distribute Candidate Information for the express limited purpose of recruitment for employment and in compliance with all applicable laws, regulations, judicial orders and Customer's privacy policy, including, but not limited to, obtaining any necessary third party consents such as opt-in consents, in connection with the Candidate Information. Customer is responsible for ensuring that all Customer Content and all use, display, and distribution thereof in connection with the Agreement each comply with applicable laws and regulations.

(d) Marks. SAP acknowledges that Customer owns certain names and logos, including, but not limited to, trademarks and trade names of its products or services. Customer's names and logos along with proprietary rights related to the same will be referred to collectively as "Marks". Subject to the terms and conditions of the Agreement and only if and as applicable, Customer hereby grants SAP a limited, nonexclusive, license to use the Marks in connection with the RM Cloud Service. SAP acknowledges that Customer is the sole owner of its Marks.

(e) Privacy Policy. Customer's consumer-facing privacy policy shall provide for the following:

(i) a provision stating that third party cookies may be placed by service providers, such as SAP, on Customer's website(s); and

(ii) a provision stating that Customer may share anonymous/aggregate information with third parties, such as SAP, for purposes relating to the RM Cloud Service.

(f) Media Spend Management. The following applies in the event Customer subscribes to Media Spend Management – Recruiter Licenses and/or Media Spend Management – Postings:

For commissionable media sources managed by SAP, SAP's media agency fee will be paid by the applicable media source. For non-commissionable media sources managed by SAP, SAP will mark-up the actual media spend at the current standard agency rate (17.65% net markup). For all managed media sources, minimum monthly commissions per media source may apply.

Customer authorizes SAP to represent it as the Agency of Record ("AOR") to 3rd party interactive media sources in relation to the Customer's sponsored recruiting advertising in order to receive commission and to allow SAP to purchase interactive media on behalf of Customer. If a 3rd party interactive media source requires a separate legal arrangement, the AOR designation does not provide SAP with the authorization to enter into any additional agreements without Customer signature.

Upon termination or expiration of any Order Form, all media source contracts entered into by SAP on Customer's behalf with Customer's authorization shall either continue at the contracted fee or, at Customer's option, be transferred, contingent upon approval of any third parties in interest, to the entity designated by Customer, or cancelled by SAP, if possible. If Customer properly terminates an Order

Form, pursuant to the terms of the Agreement, after the start of SAP-designed media campaign(s), then an early termination fee of fifteen percent (15%) of expected media spend under the campaign(s) will apply. If Customer also terminates the media campaign, then Customer will be liable for any cancellation fees charged by the applicable vendors. Notwithstanding any termination, SAP shall be entitled to be paid for all media planned or placed for Customer prior to the effective date of termination so long as such media planning and/or placement has been requested and approved by Customer.

The third party media source shall be responsible for determination, collection and remittance of all applicable taxes. SAP shall pass through to Customer any applicable taxes due by Customer without validating the appropriateness of the tax amount or providing any representations regarding the taxation of third party media products, including the treatment of such products as taxable or non-taxable by any state or local jurisdiction.

3.3. Learning and Validated Learning Cloud Services

(a) Types of Authorized Users. If and as set forth in an Order Form, the following shall apply:

(i) An External Active Authorized User is defined as a Learning or Validated Learning Cloud Service Authorized User who is not an employee of Customer, but who is maintained in the same Learning or Validated Learning Cloud Service instance. External Active Authorized Users must be identified in the Learning or Validated Learning Cloud Service by Customer separately from other Authorized Users.

(ii) For Transactional Active Authorized Users, "Transaction" means: (i) each instance that a non-employee Learning or Validated Learning Cloud Service Authorized User enrolls or is enrolled by a third party, in an instructor-led training event or offering; or (ii) each instance that a non-employee Learning or Validated Learning Cloud Service Authorized User enrolls in, is enrolled in by a third party or initially launches, an online training event or offering that will be charged. There will be no fee associated with each subsequent time that a non-employee Learning or Validated Learning Cloud Service Authorized User re-enters a course or each time a non-employee Learning or Validated Learning Cloud Service Authorized User launches a content object that comprises an online item.

(iii) For Activity-based Authorized Users, notwithstanding anything to the contrary in the Agreement, an Activity-based Authorized User means a Learning or Validated Learning Cloud Service Authorized User who, at any time during the applicable subscription year: (i) has had a learning event recorded; (ii) has had an item assignment made; (iii) is enrolled or waitlisted for a learning offering; (iv) has launched online content; or (v) has launched or attended a virtual learning system event.

(iv) A Limited Active Authorized User is defined as a Learning or Validated Learning Cloud Service Authorized User who is an employee of Customer and who takes no more than three (3) courses (e-learning or classroom) per subscription year. Limited Active Authorized Users must be identified in the Learning or Validated Learning Cloud Service by Customer separately from other Authorized Users.

(b) SAP SuccessFactors Learning, content storage. Content storage is included as part of Customer's standard subscription to the Learning or Validated Learning Cloud Service, but not included as part of a subscription to any of the additional Authorized User types described in Section 3.3.(a) above.

(i) Content storage included with the Learning or Validated Learning Cloud Service includes content bandwidth and twenty five (25) Gigabytes (GBs) of eLearning content storage. Content bandwidth is calculated based on two hundred and fifty (250) Megabytes (MBs) per (active) Authorized User per year. In the event Customer exceeds the amount of content bandwidth set forth herein, Customer may subscribe to additional GBs of bandwidth, in one hundred (100) GB increments, at SAP's then current prices, prorated for the then current subscription year, by signing an addendum to the applicable Order Form. In the event Customer exceeds the amount of content storage set forth herein, Customer may subscribe to additional GBs of storage, in twenty five (25) GB increments, at SAP's then current prices, prorated for the then current subscription year, by signing an addendum to the applicable Order Form. The increased bandwidth and/or storage levels, as applicable, will also be used for calculating the fees for any subsequent years in the Subscription Term.

(ii) Content storage includes infrastructure, including web server and disc space, and uses Akamai as the Content Delivery Network (CDN) provider. If Customer cannot support Akamai as its CDN, Content storage cannot be provisioned to Customer.

(iii) Content is not dependent on server-side software (databases, server side scripts).

(iv) Content is backed-up nightly.

(c) SAP SUCCESSFACTORS LEARNING, content service add-on. If Customer is purchasing SAP SuccessFactors Learning, content service add-on as set forth in an Order Form, the following terms shall apply.

(i) Definitions.

A. "Custom Content" means Customer-specific content created by Customer or an external developer/vendor. Content in this category is in standard e-learning format and communicates with the Learning or Validated Learning Cloud Service via the AICC or SCORM communication standards.

B. "Non-Tracking Content" means content that does not have inherent tracking capabilities per the AICC or SCORM communication standards, but can still be configured for online access through the Learning or Validated Learning Cloud Service.

C. "External Vendor Content" means generic, off the shelf, content created by a third-party content vendor. Under the assumption that the underlying code and structure is the same for all content from a particular vendor, SAP personnel will load, verify set-up and support all content, but will only validate a subset (ten percent (10%)) thereof.

(ii) Description of SuccessFactors Learning, content service add-on.

A. Content Deployment Support

(1) Customer's authorized content owners may upload courses to the SAP SuccessFactors Learning, content service add-on portal for management by the SAP SuccessFactors Learning, content service add-on service. Courses will be deployed to the SAP SuccessFactors Learning, content service add-on hosting platform, set up and tested in Customer's Learning or Validated Learning Cloud Service.

(2) SAP is responsible for testing and verification of launch, play and tracking of the Custom Content and External Vendor Content to ensure such content is communicating correctly with the Learning or Validated Learning Cloud Service, per the AICC or SCORM (including SCORM 2004) communication standards. Non-Tracking Content is tested for such content launches. All External Vendor Content is tested for launch, but only ten percent (10%) of External Vendor Content is validated for communication with the Learning or Validated Learning Cloud Service.

(3) SAP will discuss/review communication compliance issues with the content owner/creator. Customer will provide a designated contact for the Custom Content and/or Non-Tracking Content on delivery of such content to SAP.

(4) Customer will approve all content before it is pushed for live access to Customer's production environment.

(5) Ongoing updates/maintenance for all content will include:

- o Receipt of new content file from Customer, or vendor on its behalf.
- o Updating content, content object and pertinent contextual data for approval in Customer's staging and production environments.
- o Testing content for launch and, where applicable, integration with the Learning or Validated Learning Cloud Service.

B. Service Level Objective

(1) Customer will provide an appropriate level sponsor ("Project Sponsor") to provide SAP with reasonable access to business and technical contacts, background information, data and system sources, as needed, to fulfill Customer's responsibilities.

(2) Customer may designate up to two (2) authorized account contacts for the purpose of reporting content issues, defects and suggesting enhancements through their dedicated SAP SuccessFactors Learning, content service add-on consultant. For clarity, SAP will provide dedicated SAP

SuccessFactors Learning, content service add-on support to these two (2) authorized contacts. Customer, not SAP, will provide support directly to its Authorized Users.

(3) Customer may designate up to ten (10) authorized content owners who are permitted to submit content to be managed by SAP SuccessFactors Learning, content service add-on.

(4) A content upload/update of a single course will be completed within one (1) business day of SAP's receipt of any such content, through the agreed upon channels. If content validation activities indicate issues with content launch, exit or tracking (for trackable content), SAP will provide an issue report to the content owner within one (1) business day of receipt. Once the content owner has resolved the reported issue and delivers a revised version of the content to SAP, content upload and update will be completed within one (1) business day of SAP's receipt of the revised content. For clarity, this provision applies to all of the content types defined above.

(5) Any content upload/update of multiple course titles in a single day will be completed in a timeline to be mutually agreed to between the SAP SuccessFactors Learning, content service add-on consultant and an authorized account contact for Customer.

C. Assumptions and Additional Conditions

(1) Specific Customer SAP SuccessFactors Learning, content service add-on details may be defined in an Order Form. Changes to Customer's SAP SuccessFactors Learning, content service add-on subscription or service level objectives are managed via a change notification process that will require Customer signature.

(2) Content is not dependent on server-side software (databases, server side scripts).

(3) As part of SAP SuccessFactors Learning, content service add-on, SAP utilizes Akamai as its Content Delivery Network (CDN) provider. If Customer cannot support Akamai as its CDN provider, SAP SuccessFactors Learning, content service add-on cannot be provisioned to Customer.

(4) Only content that is hosted on the SAP SuccessFactors Learning, content service add-on servers is subject to the applicable support and services described herein.

(5) A single course may include up to ten (10) content objects (modules). A course that contains more than ten (10) content objects will count as multiple courses with respect to the SAP SuccessFactors Learning, content service add-on limits and, as applicable, the service level objectives described above.

(6) All courses that are active in the production instance of Customer's Learning or Validated Learning Cloud Service are included in the total course count for purposes of the SAP SuccessFactors Learning, content service add-on limits.

(7) Customer may deactivate and replace up to thirty percent (30%) of SAP SuccessFactors Learning, content service add-on supported courses during a Subscription Term.

(8) Unless otherwise expressly specified, SAP SuccessFactors Learning, content service add-on SAP SuccessFactors Learning, content service add-on does not include support or services related to the SAP SuccessFactors mobile application or offline player environments.

(9) Customer can request testing in up to three (3) different browser environments. These environments must be supported environments for Customer's version of the Learning or Validated Learning Cloud Service.

(10) Content is backed-up nightly.

3.4 Employee Central Cloud Service

(a) Employee Central Non-Employee. If Customer subscribes to Employee Central Non-Employee the following shall apply:

Employee Central Non-Employee is available for any active non-employee Authorized User whose information will be stored in the Employee Central Cloud Service, for example, retirees, contractors and contingent workers. For purposes of clarity, Employee Central Non-Employee is not available for any Authorized User who is a Full-Time or Part-Time employee.

(b) Custom Metadata Framework (MDF) Objects. When Customer subscribes to the Employee Central Cloud Service, Customer will be able to create up to twenty-five (25) custom MDF objects.

(c) If Customer receives Launch Optimization Services with the Employee Central Cloud Service, such services are described at the following link: <http://www.sap.com/corporate-en/about/our-company/policies/cloud/service-specifications.html> under "Launch Optimization Service Description". A copy will also be provided to Customer upon request.

(d) HANA Cloud Integration and Boomi Technology. If Customer subscribes to the Employee Central Cloud Service, Customer may elect to use either SAP HANA Cloud Integration or Boomi Technology as the integration middleware. The election shall be reflected on the Order Form and shall be in effect for the term of the subscription to Employee Central. If Customer elects to use SAP HANA Cloud Integration, the terms set forth in the SAP HANA Cloud Integration Supplemental Terms and Conditions shall apply, which terms can be found at SAP.com/Agreements (a copy will also be provided to Customer upon request). Notwithstanding any term in the SAP HANA Cloud Integration Supplemental Terms and Conditions, Customer may use SAP HANA Cloud Integration to connect SAP SuccessFactors Performance & Goals, SAP SuccessFactors Compensation, SAP SuccessFactors Succession & Development, SAP SuccessFactors Learning, SAP SuccessFactors Onboarding, SAP SuccessFactors Recruiting, SAP Jam (advanced edition), SAP SuccessFactors Workforce Analytics & Planning and SAP SuccessFactors Employee Central to an unlimited number of SAP cloud, on-premise or third-party solutions.

3.5 Onboarding Cloud Service

E-Verify (Applicable for US based customers only). If the Onboarding Cloud Service described in the applicable Order Form includes E-Verify, Customer must sign a separate Memorandum of Understanding ("MOU") between the United States Department of Homeland Security, Customer, and SAP's affiliate, SuccessFactors, Inc., designating SuccessFactors, Inc. as its Web Services E-Verify Employer Agent. Customer shall be responsible for complying with all terms of the MOU related to Customer. Customer's failure to comply with the MOU might affect SAP's ability to provide E-Verify with the Onboarding Cloud Service, and SAP shall be excused from any such failure to perform. Customer's failure to comply with the MOU shall not relieve Customer of its payment obligations under the Agreement.

Appendix 1

Package and Product Descriptions

PACKAGES

In addition to the Products identified below, each of the Packages listed below includes SuccessFactors Foundation. SuccessFactors Foundation comprises the following: Employee Profile, SAP Jam (basic edition), Talent Insights, Job Profile Builder and SuccessFactors asynchronous, digital web-based Administrator training.

1. SAP SuccessFactors Advanced Learning

The SAP SuccessFactors Advanced Learning Package comprises the following Products: SAP SuccessFactors Succession & Development, SAP SuccessFactors Learning and SAP Jam (advanced edition).

2. SAP SuccessFactors Perform & Reward

The SAP SuccessFactors Perform & Reward Package comprises the following Products: SAP SuccessFactors Performance & Goals and SAP SuccessFactors Compensation.

3. SAP SuccessFactors Talent Management

The SAP SuccessFactors Talent Management Package comprises the following Products: SAP SuccessFactors Performance & Goals, SAP SuccessFactors Compensation, SAP SuccessFactors Succession & Development, SAP SuccessFactors Learning, SAP SuccessFactors Recruiting and SAP Jam (advanced edition).

4. SAP SuccessFactors Enterprise basic

The SAP SuccessFactors Enterprise basic package comprises the following Products: SAP SuccessFactors Performance & Goals, SAP SuccessFactors Compensation, SAP SuccessFactors Succession & Development, SAP SuccessFactors Learning, SAP SuccessFactors Recruiting, SAP Jam (advanced edition), SAP SuccessFactors Workforce Analytics & Planning and SAP SuccessFactors Employee Central.

5. SAP SuccessFactors Enterprise

The SAP SuccessFactors Enterprise Package comprises the following Products: SAP SuccessFactors Performance & Goals, SAP SuccessFactors Compensation, SAP SuccessFactors Succession & Development, SAP SuccessFactors Learning, SAP SuccessFactors Onboarding, SAP SuccessFactors Recruiting, SAP Jam (advanced edition), SAP SuccessFactors Workforce Analytics & Planning and SAP SuccessFactors Employee Central.

PRODUCTS

In addition to the modules identified below, each of the Products listed below, **except for SAP Jam, and SAP SuccessFactors Employee Central Payroll**, includes SuccessFactors Foundation. SuccessFactors Foundation comprises the following: Employee Profile, SAP Jam (basic edition), Talent Insights, Job Profile Builder and SuccessFactors asynchronous, digital web-based Administrator training.

1. SAP SuccessFactors Performance & Goals

The SAP SuccessFactors Performance & Goals Product comprises Performance Management, Goals Management, 360 Degree Reviews, Stack Ranker and Calibration (for Performance).

2. SAP SuccessFactors Compensation

The SAP SuccessFactors Compensation Product comprises SAP SuccessFactors Compensation, Calibration (for Compensation) and Variable Pay.

3. SAP SuccessFactors Succession & Development

The SAP SuccessFactors Succession & Development Product comprises Succession Planning, Career & Development Planning and Calibration (for Talent).

4. SAP SuccessFactors Learning

The SAP SuccessFactors Learning Product comprises SAP SuccessFactors Learning.

5. SAP SuccessFactors Validated Learning

The SAP SuccessFactors Validated Learning Product comprises SAP SuccessFactors Validated Learning.

6. SAP SuccessFactors Employee Central

The SAP SuccessFactors Employee Central Product comprises SAP SuccessFactors Employee Central and either SAP HANA Cloud Integration or Boomi Technology.

7. SAP SuccessFactors Employee Central Payroll

The SAP SuccessFactors Employee Central Payroll Product comprises Employee Central Payroll.

8. SAP SuccessFactors Onboarding

The SAP SuccessFactors Onboarding Product comprises SAP SuccessFactors Onboarding.

9. SAP SuccessFactors Recruiting

The SAP SuccessFactors Recruiting Product comprises SAP SuccessFactors Recruiting Management and SAP SuccessFactors Recruiting Marketing.

10. SAP SuccessFactors Recruiting Marketing

The SAP SuccessFactors Recruiting Marketing Product comprises SAP SuccessFactors Recruiting Marketing.

11. SAP SuccessFactors Recruiting Management

The SAP SuccessFactors Recruiting Management Product comprises SAP SuccessFactors Recruiting Management.

12. SAP SuccessFactors Workforce Analytics & Planning Product

The SAP SuccessFactors Workforce Analytics & Planning Product comprises SAP SuccessFactors Workforce Analytics and SAP SuccessFactors Workforce Planning.

13. SAP SuccessFactors Workforce Planning Product

The SAP SuccessFactors Workforce Planning Product comprises SAP SuccessFactors Workforce Planning.

14. SAP SuccessFactors Workforce Analytics Product

The SAP SuccessFactors Workforce Analytics Product comprises SAP SuccessFactors Workforce Analytics.

15. SAP Jam

The SAP Jam Product comprises SAP Jam, available in basic, advanced, advanced plus or enterprise edition.

MISCELLANEOUS

1. Perform & Reward for Small Business: SAP Perform & Reward for Small Business comprises Performance Management (no Calibration), Goal Management (no Goal Execution), Employee Profile, 360 Degree Reviews, Stack Ranker, Reports & Dashboards and Compensation Management (no Calibration, no Variable Pay).

2. SAP SuccessFactors Employee Central Service Center: SAP SuccessFactors Employee Central Service Center comprises SAP HANA Cloud Portal and SAP Cloud for Service (including SAP Cloud Applications Studio). For each three hundred (300) Employees subscribed to in an Order Form, Customer may have one user acting as a service agent to access SAP SuccessFactors Employee Central Service Center. A subscription to SAP SuccessFactors Employee Central is a prerequisite to a subscription to SAP SuccessFactors Employee Central Service Center. Support terms, Service Availability and Maintenance Windows for SAP HANA Cloud Portal are found in the SAP HANA Cloud Portal Supplemental Terms and Conditions (available from SAP upon request). Maintenance Windows for SAP Cloud for Service and the terms governing use of the SAP Cloud Applications Studio and Mobile Access are found in the SAP Cloud for Customer Supplemental Terms and Conditions (available from SAP upon request).

3. SAP HANA Cloud Platform, extension package for SuccessFactors: If Customer elects to subscribe to SAP HANA Cloud Platform, extension package for SuccessFactors, the terms set forth in the SAP HANA Cloud Platform Supplemental Terms and Conditions (available from SAP upon request) shall apply.

SUPPORT POLICY FOR SAP CLOUD SERVICES

Effective April 15, 2015, to further align its support offerings across all solutions and deployment options consistent with SAP's ONE Support approach, SAP has further evolved its support offerings to two SAP Cloud Service support levels, SAP Enterprise Support, cloud editions and SAP Preferred Care. As part of SAP's ONE Support approach with SAP's support for Cloud Services and on-premise solutions, SAP focuses its support services on four principles: mission critical support, empowerment, collaboration and innovation and value realization.

SUPPORT OFFERINGS

SAP Enterprise Support, cloud editions is included in the subscription fees for most SAP Cloud Services. Customers may check if SAP Enterprise Support, cloud editions is part of their specific SAP Cloud Service by assessing their Supplement referenced in the Order Form. For an additional fee, customers can obtain SAP Preferred Care as an add-on to complement SAP Enterprise Support, cloud editions, if and when available, for the applicable SAP Cloud Services.

SAP account executives or SAP partners can assist in case of questions related to these new support offerings.

The following table describes the services included in SAP Enterprise Support, cloud editions and SAP Preferred Care. Further clarification of terms in the following table is provided in the Capitalized Terms table below.

	SAP Enterprise Support, cloud editions	SAP Preferred Care
Description	Embedded engagement support with focus on customer interaction and issue resolution.	An add-on to SAP Enterprise Support, cloud editions that includes a high touch model with focus on strategic guidance and individualized best practices to drive user adoption and value realization (Representation below includes SAP Enterprise Support, cloud editions).
Mission Critical Support		
24x7 Mission Critical Support for P1 and P2 issues (English only)	✓	24x7 prioritized issue handling
Non-Mission Critical Support for P3 and P4 issues (English only) during business hours	Monday to Friday 8 am to 6 pm (Local Time Zone), excluding local holidays	Monday to Friday 8 am to 6 pm (Local Time Zone), excluding local holidays
Customer Interaction Center 24x7	English	In available languages as set forth below
Global Support Backbone	✓	✓
End-to-end Supportability in hybrid SAP landscapes	✓	✓
Release Weekend Support by Customer Success Manager		Currently available for SAP SuccessFactors Cloud Service. SAP may make this available for additional SAP Cloud Services in its sole discretion
Empowerment		
Access to the SAP Enterprise Support Academy	✓	✓

Meet-the-Expert Sessions	✓	✓
Release Update Information	Self-serve through web and community	Personalized Release Update Information adjusted to customer's environment
Collaboration		
Access to SAP Support Advisory Center expert pool	✓	✓
SAP Cloud Service and process-related guidance		Designated Customer Success Manager for technical and product usage advisement, best practices and operational excellence (within customer's region), and personalized advice and guidance for human resource cycles related to performance, goal management and compensation
Weekly checkpoint		Meeting with customer to review issues tracking, reporting and guidance and best practices
Support via web and platform for social business collaboration	✓	✓
Support via chat during business hours in English language for non-Mission Critical Support issues, as made available by SAP	Currently available for SAP SuccessFactors Cloud Service. SAP may make this available for additional SAP Cloud Services in its sole discretion.	Currently available for SAP SuccessFactors Cloud Service. SAP may make this available for additional SAP Cloud Services in its sole discretion.
SAP Enterprise Support Report Cloud Edition	✓	✓
Innovation and Value Realization		
Proactive checks proposed by SAP to optimize implementation	✓	✓
Product Roadmap Update Information	Self-serve through web and community	Personalized Product Roadmap Update Information, as requested, adjusted to customer's environment
Periodic account review and planning		Onsite meeting with customer to discuss checkpoint, cycle planning, challenges and adoption plan
Monitoring Components	✓	✓
Refresh of Test Instance	Self-service through web for initiating the refreshing of customer test instance up to two times per year	Personalized assistance with managing the refreshing of test instances up to two times per year

Empowerment content and session schedules are stated at the SAP Support Portal under the [SAP Enterprise Support Academy](#) section. Scheduling, availability and delivery methodology is at SAP's discretion.

SAP Enterprise Support, cloud editions support related to Empowerment and Innovation and Value Realization as stated above, shall require a customer request and shall be provided remotely. For example, remote support services may include assisting customers in evaluating the innovation capabilities of the latest updates and technology innovation and how it may be deployed for a

customer's business process requirements, or giving customer guidance in form of knowledge transfer sessions. Scheduling, availability and delivery methodology is at SAP's discretion.

LANGUAGES

SAP, through the 'OneSAP' support phone number "CALL-1-SAP" (stated at the SAP Support Portal <https://support.sap.com/support-programs-services/programs/one-support-program.html>), provides multi-language support for SAP telephone-support inquiries in the following languages: English; German, available during the above support hours of operation for Germany; Spanish, available during the above support hours of operation for Spain, Latin America, Central America and Caribbean countries; French, available during the above support hours of operation for France and Quebec, Canada; Chinese (Mandarin), available during the above support hours of operation for China; Japanese, available during the above support hours of operations for Japan; and Portuguese, available during the above support hours for Brazil. Customers may receive technical resolution support in the non-English languages specified above by contacting SAP's support organization for the above applicable countries. Any support by a third party or by SAP outside of the designated call centers for the multi-language support described in this paragraph is in English only.

CONTACTING SUPPORT

Beginning on the effective date of a customer's agreement for Cloud Services, that customer may contact SAP's support organization as primary point of contact for support services.

For contacting SAP's support organization, the current preferred contact channels for SAP Enterprise Support, cloud editions are set forth in the table below.

SAP Cloud Service	Contact Channels
SAP SuccessFactors Cloud Service	SAP Support Portal at https://support.sap.com .
SAP Business ByDesign SAP Cloud for Customer	Embedded in the applicable SAP Cloud Service: <ul style="list-style-type: none"> • For end-users: The "Help Center", accessible from every screen, • For Key Users: The "Application & User Management Work Center". In addition: "Business Center for Cloud Solutions" at http://businesscenter.sap.com/ .

Customers that have subscribed to the SAP Preferred Care services may contact SAP directly through the assigned Customer Success Manager.

CUSTOMER RESPONSE LEVELS

SAP responds to submitted support cases (also referred to as "case", "incident", or "issue") as described in the table below.

Priority	Definition	Response Level
P1	<p>Very High: An incident should be categorized with the priority "very high" if the problem has very serious consequences for normal business processes or IT processes related to core business processes. Urgent work cannot be performed.</p> <p>This is generally caused by the following circumstances:</p> <ul style="list-style-type: none"> - A productive service is completely down. - The imminent system Go-Live or upgrade of a production system cannot be completed. - The customer's core business processes are seriously affected. <p>A workaround is not available for each circumstance.</p> <p>The incident requires immediate processing because the malfunction may cause serious losses. In case of a Go-Live or upgrade, the reason to delay the Go-Live or upgrade must be one that would cause serious losses if not resolved before Go-Live.</p>	<p>Initial Response: Within one hour of case being submitted.</p> <p>Ongoing Communication: Once every hour, unless otherwise communicated by SAP Support.</p> <p>Resolution Target: SAP to provide for issues either a (i) resolution, or (ii) workaround or (iii) action plan within 4 hours.</p>
P2	<p>High: An incident should be categorized with the priority "high" if normal business processes are seriously affected. Necessary tasks cannot be performed. This is caused by incorrect or inoperable functions in the SAP service that are required immediately.</p> <p>The incident is to be processed as quickly as possible because a continuing malfunction can seriously disrupt the entire productive business flow.</p>	<p>Initial Response: Within four hours of case being submitted for SAP Enterprise Support, cloud edition customers and within two hours of case being submitted for SAP Preferred Care customers.</p> <p>Ongoing Communication: Once every six hours unless otherwise communicated by SAP Support.</p> <p>Resolution Target: SAP to provide for issues either a (i) resolution, or (ii) workaround or (iii) action plan within three business days for SAP Preferred Care customers only.</p>
P3	<p>Medium: An incident should be categorized with the priority "medium" if normal business processes are affected. The problem is caused by incorrect or inoperable functions in the SAP service.</p>	<p>Initial Response: Within one business day of case being submitted for SAP Enterprise Support, cloud edition customers, and within four business hours of case being submitted for SAP Preferred Care customers.</p> <p>Ongoing Communication: Once every three business days for Non-Defect Issues and 10</p>

business days for product defect issues unless otherwise communicated by SAP Support.

P4 **Low:** An incident should be categorized with the priority "low" if the problem has little or no effect on normal business processes. The problem is caused by incorrect or inoperable functions in the SAP service that are not required daily, or are rarely used.

Initial Response: Within two business days of case being submitted for SAP Enterprise Support, cloud edition customers and within one business day of case being submitted for SAP Preferred Care customers.

Ongoing Communication: Once every week unless otherwise communicated by SAP's support organization.

The following types of incidents are excluded from customer response levels as described above: (i) incidents regarding a release, version and/or functionalities of SAP Cloud Services developed specifically for customer (including without limitation those developed by SAP Custom Development and/or by SAP subsidiaries); (ii) the root cause behind the incident is not a malfunction, but a missing functionality ("development request") or the incident is ascribed to a consulting request ("how-to").

CUSTOMER'S RESPONSIBILITIES

In order to receive support hereunder, customers shall designate qualified English speaking contact persons (each a "Customer Contact" or "key user") for the SAP Support Advisory Center and Mission Critical Support.

SAP allows customers to have two primary Customer Contacts (as defined below) and two back-up Customer Contacts per Product Bundle. Only authorized Customer Contacts may contact SAP's support organization.

At least one of a customer's primary and back-up Customer Contacts shall be an application administrator. Application administrators should have taken SAP's Admin Training Course located at the SAP Support Portal under the SAP Enterprise Support Academy.

Customers shall provide contact details (in particular e-mail address and telephone number) by means of which the Customer Contact or the authorized representative of such Customer Contact can be contacted at any time. Customers shall update their Customer Contacts for an SAP Cloud Service through the SAP Support Portal at <https://support.sap.com> or the "Service Control Center" embedded in the SAP Cloud Service as applicable. SAP may, from time to time, confirm with customers the correctness of information customers provide as required herein.

To receive support services hereunder, customers shall reasonably cooperate with SAP to resolve support incidents, and shall have adequate technical expertise and knowledge of their configuration of the SAP Cloud Services to provide relevant information to enable SAP to reproduce, troubleshoot and resolve the experienced error such as, by way of an example, instance name, username, form name and screenshot.

CAPITALIZED TERMS

Below are further explanations of the capitalized terms used above:

Customer Interaction Center 24x7	A global unit within SAP’s support organization that customers may contact for general support related inquiries through the described contact channels.
Customer Success Manager	A specific SAP customer representative that is assigned as primary contact for ongoing management, provides support case oversight, technical guidance and mentorship. Provides personalized information on release updates and guidance on adoption and usage.
End-to-end Supportability	Support for incidents that occur in integrated business scenarios consisting of both SAP Cloud Services and other SAP products with a valid support agreement.
Global Support Backbone	SAP’s knowledge database and SAP’s extranet for knowledge transfer on which SAP makes available content and services to customers and partners of SAP only. The Global Support Backbone also includes the SAP Support Portal at https://support.sap.com .
Go-Live	Go-Live marks the point in time from when, after set-up of the SAP Cloud Services for the a customer, the SAP Cloud Services can be used by that customer for processing real data in live operation mode and for running that customer’s internal business operations in accordance with its agreement for such SAP Cloud Services.
Local Time Zone	A customer’s local time zone, depending on where the customer is headquartered.
Meet-the-Expert Sessions (MTE)	Live webinars focusing on SAP Enterprise Support services and the support aspects of the latest SAP technologies. Recorded sessions are available in the replay library in the SAP Enterprise Support Academy for self-paced consumption.
Mission Critical Support	Global incident handling by SAP for issues related to support hereunder with P1 and P2, including Service Level Agreements for Initial Response, Ongoing Communications and Resolution Targets (as set forth in the above table for Response Levels).
Monitoring Components	Monitoring components and agents for systems to monitor available resources and collect system status information of the SAP Cloud Services.
Non-Defect Issue	A reported support case that does not involve a defect in the applicable SAP Cloud Service and does not require engineering or operations personnel to resolve.
Product Bundle	A combination of SAP Cloud Services, if any, that a customer subscribes to as part of its order for SAP Cloud Services.
Product Roadmap Update Information	Product roadmaps SAP makes generally available to customers as part of customer support. Product Roadmap Update Information is provided for informational purposes only, and SAP does not commit to providing any future products, features or functionality as described in the Product Roadmap Update Information.
Refresh of Test Instance	Up to twice per year, upon customer’s written request, SAP will perform a refresh of customer’s test instance of the SAP Cloud Service with the then-current settings, updates and configurations to mirror customer’s production instance of the SAP Cloud Service at the time of such instance refresh.

Release Weekend Support	Customer Success Managers and the Preferred Care Leadership team will provide post release Preferred Care coverage for the weekend of a quarterly product release to address any post release P1 (Very High) and P2 (High) incidents that occur in connection with the quarterly product release.
Release Update Information	Generally available documented summaries, webinars and videos provided by SAP to inform and instruct customers on new product release changes.
SAP Cloud Service	Any SAP Cloud Service set forth in an applicable Order Form.
SAP Enterprise Support Academy	Content and services in several formats, supporting different learning styles and needs, from ad hoc problem solving to structured, long-term knowledge acquisition.
SAP Enterprise Support Report Cloud Edition	A report analyzing and documenting the status of support services and achievements hereunder.
SAP Support Advisory Center	A global unit within SAP's support organization for Mission Critical Support-related requests.

SERVICE LEVEL AGREEMENT FOR SAP CLOUD SERVICES ("SLA")

1. Service Level Agreement

This Service Level Agreement for SAP Cloud Services sets forth the System Availability SLA for the productive version of the applicable SAP Cloud Services to which customer has subscribed ("**Cloud Services**") in an Order Form with SAP.

This Service Level Agreement for SAP Cloud Services shall not apply to any SAP Cloud Service for which a System Availability service level is explicitly set forth in the applicable Supplemental Terms and Conditions for such SAP Cloud Service or for which the applicability of service levels is explicitly excluded in the Agreement.

2. Definitions

"**Downtime**" means the Total Minutes in the Month during which the productive version of the applicable Cloud Service is not available, except for Excluded Downtimes.

"**Local Time**" means, except as otherwise expressly defined in Section 4 below, the following time zones:

UTC-4, Americas (summer); UTC-5, Americas (EST winter)

UTC+2, Europe (summer); UTC+1, Europe (CET winter); UTC+8, APJ

"**Month**" means a calendar month.

"**Monthly Subscription Fees**" means the monthly (or 1/12 of the annual fee) subscription fees paid for the Cloud Service which did not meet the System Availability SLA.

"**Total Minutes in the Month**" are measured 24 hours at 7 days a week during a Month.

3. System Availability SLA and Credits

3.1 Claim process, Reports

Customer may claim a credit in the amount described in the table of Section 3.2 below in case of SAP's failure to meet the System Availability SLA, which credit Customer may apply to a future invoice relating to the Cloud Service that did not meet the System Availability SLA.

Claims under this Service Level Agreement must be made in good faith and by submitting a support case within thirty (30) business days after the end of the relevant Month in which SAP did not meet the System Availability SLA.

SAP will provide to customers a monthly report describing the System Availability percentage for the applicable Cloud Service either (i) by email following a customer's request to its assigned SAP account manager, (ii) through the Cloud Service or (iii) through an online portal made available to customers, if and when such online portal becomes available.

3.2 System Availability

System Availability percentage is calculated as follows:

$$System\ Availability\ \%age = \left[\left(\frac{Total\ Minutes\ in\ the\ Month - Downtime}{Total\ Minutes\ in\ the\ Month} \right) * 100 \right]$$

System Availability SLA ("SLA")	99.5% System Availability percentage during each Month for productive versions
Credit	2% of Monthly Subscription Fees for each 1% below SLA, not to exceed 100% of Monthly Subscription Fees
Excluded Downtime	Total Minutes in the Month attributable to: (i) a Scheduled Downtime for which a Regular Maintenance Window is described in Section 4 below, or (ii) any other Scheduled Downtime according to Section 4 for which the customer has been notified at least five (5) business days prior to such Scheduled Downtime or (iii) unavailability caused by factors outside of SAP's reasonable control, such as unpredictable and unforeseeable events that could not have been avoided even if reasonable care had been exercised.

Scheduled Downtime	Scheduled Downtime for the applicable Cloud Services to which customer has subscribed is set forth in Section 4 below entitled "Maintenance Windows for Cloud Services".
---------------------------	--

4. Maintenance Windows for SAP Cloud Services

SAP can use the following maintenance windows for Scheduled Downtimes as listed below. Where "Local Time" is referenced, this refers to the location of the data center where the SAP Cloud Service is hosted.

SAP Agile Data Management

	Maintenance Windows
Regular Maintenance Windows	Weekly Friday 5:00 p.m. to 7:00 p.m. Pacific USA Time
Major Upgrades	Up to 12 times per year from Friday 5:00 p.m. to Friday 10 mid-night Pacific USA Time

SAP Anywhere

	Maintenance Windows
Regular Maintenance Windows	Weekly Tuesdays for no more than 2 hours from 11: 00 p.m. to 3:00 a.m. Local Time, and at any time upon 5 days' notice from SAP for up to 4 hours.
Major Upgrades	None

API Management

	Maintenance Windows
Regular Maintenance Windows	Weekly, Sunday 4:00 a.m. to Sunday 6:00 a.m. Local Time.
Major Upgrades	Friday 10:00 p.m. to Monday 3:00 a.m. Local Time once per quarter. SAP will inform Customer reasonably in advance about planned major upgrade scheduling.

SAP Ariba Cloud Offerings

	Maintenance Windows
Regular Maintenance Windows	Saturday, 8:00 a.m. to Saturday, 8:00 p.m. Pacific U.S. Time

SAP reserves the right to extend or change the times of the Regular Maintenance Window for SAP Ariba Cloud Services, subject to customer rights contained in the GTC.. Notwithstanding Section 3.2 of this Service Level Agreement, SAP will use commercially reasonable efforts to notify Customers at least 72 hours prior to the occurrence of Scheduled Downtime for SAP Ariba Cloud Services.

SAP Assessment Management by Questionmark

	Maintenance Windows
Regular Maintenance Windows	Third Saturday of each month, 5:00 a.m. to 5:00 p.m. Eastern U.S. time for data center(s) located in the U.S.; and 10:00 a.m. to 10:00 p.m. GMT for data center(s) located in Europe.

SAP Browse Manager and Conversion Manager

	Maintenance Windows
Regular Maintenance Windows	Weekly, between 6:00 p.m. Friday and 3:00 a.m. Monday, U.S. Eastern Time Zone.

SAP BusinessByDesign

	Maintenance Windows
Regular Maintenance Windows	Weekly, Sunday 2:00 a.m. to Sunday 6:00 a.m. Local Time.
Major Upgrades	Up to 4 times per year from Saturday 6:00 a.m. to Sunday 6:00 a.m. Local Time.

SAP Circular Authority

	Maintenance Windows
Regular Maintenance Windows	Nightly, from 9:00 p.m. to 6:00 a.m. Eastern U.S. time.
Major Upgrades	Last Friday of each calendar month from 9:00 p.m. to Monday 6:00 a.m. Eastern U.S. time.

SAP Cloud Appliance Library

	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.
Major Upgrades – SAP HANA Cloud Platform	Up to 4 times per year from Friday 10:00 p.m. to Monday 3:00 a.m. Local Time.
SAP Cloud Appliance Library Upgrades**	Once per calendar month, during a one (1) hour window made known by SAP at least one (1) week in advance.

** Maintenance Windows for the SAP Cloud Appliance Library are separate from and in addition to Maintenance Windows for the SAP HANA Cloud, both of which are applicable to the Cloud Service.

SAP Cloud for Analytics

	Maintenance Windows
Regular Maintenance Windows	Weekly Saturday – 7:00 a.m. to 10:00 a.m. Australian Eastern Standard Time (AEST = UTC + 10) / Australian Eastern Daylight Time (AEDT = UTC+11) for data centers in Australia. Sunday – 8:00 p.m. to 11:00 p.m. Eastern Standard Time (EST =UTC-5) / Eastern Daylight Time (EDT = UTC – 4) for datacenters in Americas. Friday – 10:00 p.m. to 1:00 a.m. Saturday Central European Time (CET = (UTC+1) / Central European Summer Time (CEST = UTC+2) for data centers in Europe.
Major Upgrades	Weekly, Friday 6:00 p.m. to 9:00 p.m. Australian Eastern Standard Time (AEST = UTC + 10) / Australian Eastern Daylight Time (AEDT = UTC+11) for data centers in Australia. 5:00 a.m. to 8:00 a.m. Eastern Standard Time (EST =UTC-5) / Eastern Daylight Time (EDT = UTC – 4) for data centers in Americas. 2:00 p.m. to 5:00 p.m. Central European Time (CET = (UTC+1) / Central European Summer Time (CEST = UTC+2) for datacenters in Europe.

SAP Cloud for Customer

		Maintenance Windows
Regular Maintenance Windows		Weekly, Sunday 2:00 a.m. to Sunday 6:00 a.m. Local Time.
Major Upgrades		Up to 4 times per year from Saturday 6:00 am to Sunday 6:00 a.m. Local Time.

SAP Cloud for EPM (Includes Cloud for Planning)

		Maintenance Windows
Regular Maintenance Windows		Weekly: Saturday – 7:00 a.m. to 10:00 a.m. Australian Eastern Standard Time (AEST = UTC + 10) / Australian Eastern Daylight Time (AEDT = UTC+11) for data centers in Australia. Sunday – 8:00 p.m. to 11:00 p.m. Eastern Standard Time (EST =UTC-5) / Eastern Daylight Time (EDT = UTC – 4) for datacenters in Americas. Friday – 10:00 p.m. to 1:00 a.m. Saturday Central European Time (CET = (UTC+1) / Central European Summer Time (CEST = UTC+2) for data centers in Europe.
Major Upgrades		Weekly, Friday: 6:00 p.m. to 9:00 p.m. Australian Eastern Standard Time (AEST = UTC + 10) / Australian Eastern Daylight Time (AEDT = UTC+11) for data centers in Australia. 5:00 a.m. to 8:00 a.m. Eastern Standard Time (EST =UTC-5) / Eastern Daylight Time (EDT = UTC – 4) for data centers in Americas. 2:00 p.m. to 5:00 p.m. Central European Time (CET = (UTC+1) / Central European Summer Time (CEST = UTC+2) for datacenters in Europe.

SAP Cloud for Product Stewardship

		Maintenance Windows
Regular Maintenance Windows		Bi-Weekly, Thursday 11:00 a.m. to Thursday 11:45 a.m. Local Time.
Major Upgrades		Up to 4 times per year from Thursday 11:00 a.m. to Friday 11:00 a.m. Local Time.

SAP Cloud for Travel and Expense

		Maintenance Windows
Regular Maintenance Windows		Weekly, Sunday 2:00 a.m. to Sunday 6:00 a.m. Local Time.
Major Upgrades		Up to 4 times per year from Saturday 6:00 a.m. to Sunday 6:00 a.m. Local Time.

SAP Communication Center by Ancile

	Maintenance Windows
Regular Maintenance Windows	Customer may select from any one of the following maintenance window options: (1) Tuesday and Thursday from 2:00 a.m. to 4:00 a.m. Local Time (*); or (2) Saturday from 2:00 a.m. to 6:00 a.m. Local Time.
Major Upgrades	Up to 4 times per year from Friday 10:00 p.m. to Saturday 10:00 p.m. Local Time.

SAP Connected Logistics

	Maintenance Windows
Regular Maintenance Windows	Weekly, Monday and Thursday morning 4:30 a.m. to 6:30 a.m. Central European Time (CET).
Major Upgrades	Up to 4 times per year on any weekday from 4:30 a.m. to 8:30 a.m. Central European Time (CET).

SAP Contact Center, Cloud Edition

	Maintenance Windows
Regular Maintenance Windows	Weekly, Wednesday 1:00 a.m. – 5:00 a.m. Local Time
Major Upgrades	Quarterly, Friday 10:00 p.m. – Monday 3:00 a.m.

SAP Event Ticketing, SAP Event Ticketing Pro

	Maintenance Window
Regular Maintenance Windows	From midnight to 6:00 a.m. Mondays and Wednesdays, Local Time.
Major Upgrades	Max. 2 per year from 10:00 p.m. on a Friday to 4:00 a.m. on a Monday, Local Time.

SAP Financial Services Network

	Maintenance Windows
Regular Maintenance Windows	Weekly, Sunday 4:00 a.m. to Sunday 6:00 a.m. Local Time.
Major Upgrades	Up to 4 times per year from Friday 10:00 p.m. to Monday 3:00 a.m. Local Time.

HANA Cloud Integration

	Maintenance Windows
Regular Maintenance Windows	Weekly, Sunday 4:00 a.m. to 6:00 a.m. Local Time.
Major Upgrades	Quarterly, Friday 10:00 p.m. to Monday 3:00 a.m. Local Time.

HANA Cloud Platform

	Maintenance Windows
Regular Maintenance Windows	Platform: Bi-weekly, in odd calendar weeks (e.g., calendar week 1, 3, 5, etc.), Thursday morning 7AM to 8AM CET. SAP HANA Cloud Portal: Bi-weekly, in odd calendar weeks, Sundays 12:00 -13:00 CET.
Major Upgrades	Up to 4 times per year from Friday 10 pm to Monday 3 am Coordinated Universal Time(*).SAP will inform Customer in due time in advance (either by email or by any other electronic means)

HANA Cloud Platform gamification service

	Maintenance Windows
Regular Maintenance Windows	Bi-weekly, in odd calendar weeks (e.g., calendar week 1, 3, 5, etc.) during the following times: For data centers in Europe: Thursday morning 7:00 a.m. to 8:00 a.m. Central European Time (CET) = UTC+1) / Central European Summer Time (CEST = UTC+2) , For data centers in the United States: 3:00 a.m. to 4:00 a.m. Eastern Standard Time (EST = UTC-5) / 4:00 a.m. to 5:00 a.m. Eastern Daylight Time (EDT = UTC-4) For data centers in Australia: 10:00 p.m. to 11:00 p.m. Australian Eastern Standard Time (AEST = UTC+10) / 11:00 p.m. to 12:00 a.m. Australian Eastern Daylight Time (AEDT = UTC+11). In this downtime Platform Applications cannot be deployed and re-started. Running Platform Applications will not be affected.
Major Upgrades	Up to 4 times per year from Saturday 8:00 a.m. to 2:00 p.m. Central European Time (CET). SAP will inform Customer in due time in advance (either by email or by any other electronic means).

SAP Consumer Insight 365

	Maintenance Windows
Regular Maintenance Windows	Weekly, Friday 8:00 p.m. – Monday 8:00 a.m. U.S. Eastern Time
Major Upgrades	Quarterly, Friday 8:00 p.m. – Monday 8:00 a.m. Eastern Time

SAP Fiori, cloud edition

	Maintenance Windows
Regular Maintenance Windows	Bi-weekly, in odd calendar weeks (e.g., calendar week 1, 3, 5, etc.), Thursday 9:00 a.m. to 11:00 a.m. CET.
Major Upgrades	Up to 4 times per year from Saturday 8:00 a.m. to 2:00 p.m. CET (*). SAP will inform Customer in due time in advance (either by email or by any other electronic means)

SAP Innovation Management

	Maintenance Windows
Regular Maintenance Windows	Weekly, Sunday 4 AM to 6 AM Local Time.
Major Upgrades	Quarterly, Friday 10PM to Monday 3AM

SAP Integrated Business Planning (formerly SAP Sales & Operations Planning)

	Maintenance Windows
Regular Maintenance Windows	Weekly, Sunday 2:00 a.m. to 6:00 a.m. Local Time.
Major Upgrades	Friday 10:00 p.m. to Monday 3:00 a.m. Local Time once per quarter.
Minor Upgrades	Sunday 2:00 a.m. to 2:00 p.m. Local Time once per quarter.

SAP Knowledge Central by Mindtouch

	Maintenance Windows
Regular Maintenance Windows	SAP may use one of the following maintenance window options: (1) Tuesday and Thursday from 2:00 a.m. to 4:00 a.m. Local Time; or (2) Saturday from 2:00 a.m. to 6:00 a.m. Local Time.
Major Upgrades	Up to 4 times per year from Friday 10:00 p.m. to Saturday 10:00 p.m. Local Time.

SAP Lumira Cloud

	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.
Major Upgrades	Up to 4 times per year from Friday 10:00 p.m. to Monday 3:00 a.m. Local Time (*)

SAP Mobile Secure Cloud Edition

	Maintenance Windows
Regular Maintenance Windows	Bi-weekly, in odd calendar weeks (e.g., calendar week 1, 3, 5, etc.), Saturday 2:00 a.m. to 10:00 a.m. Eastern U.S. time.
Major Upgrades	Up to 4 times per year from Friday 10:00 p.m. to Monday 3:00 a.m. Local Time.

SAP Precision Marketing

	Maintenance Windows
Regular Maintenance Windows	Bi-weekly, Wednesday morning 4:00 a.m. to 6:00 a.m. Central European Time (CET).
Major Upgrades	Up to 4 times per year from Friday 10:00 pm to Monday 3:00 a.m. Local Time.

SAP Predictive Maintenance and Service. Cloud Edition

	Maintenance Windows
Regular Maintenance Windows	Weekly Friday 4:00 p.m. to 6:00 p.m. Central European Time (CET).
Major Upgrades	Up to 8 times per year from Friday 4:00 p.m. to Monday 8:00 a.m. CET.

SAP Product Stewardship Network

	Maintenance Windows
Regular Maintenance Windows	Tuesdays and Thursdays from 8:00 a.m. to 9:00 a.m. Central European Time (UTC+1) or CEST in summer time (UTC+2).
Major Upgrades	Up to 4 times per year from Tuesday 5:00 a.m. to Tuesday 12:00 p.m. Central European Time. SAP will inform Customer reasonably in advance about planned major upgrade scheduling.
Emergency Maintenance	Only as required for emergency fixes, any day of the week, if possible from 8:00 a.m. to 9:00 a.m. Central European Time (UTC+1), or CEST in summer time (UTC+2). SAP will notify customers as soon as possible when an emergency maintenance window is planned.

SAP Resolve

	Maintenance Windows
Regular Maintenance Window	Third Saturday of each month, 9:00 p.m. to 11:00 p.m. Eastern Standard Time (EST =UTC-5) / Eastern Daylight Time (EDT = UTC - 4)
Major Upgrades	Up to four times per year from Friday 10:00 p.m. to Monday 3:00 a.m. Eastern Standard Time (EST =UTC-5) / Eastern Daylight Time (EDT = UTC - 4)

S/4HANA Cloud Edition

	Maintenance Windows
Regular Maintenance Windows	Weekly, Sunday 2:00 a.m. to Sunday 6:00 a.m. Local Time.
Major Upgrades	Up to 4 times per year from Friday 10:00 p.m. to Monday 3:00 a.m. Local Time.

SAP Scouting

	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.
Major Upgrades	Up to 4 times per year from Friday 10:00 p.m. to Monday 3:00 a.m. Local Time.

SAP Sentinel cloud edition

	Maintenance Windows
Regular Maintenance Windows	Daily, 3:00 a.m. to 6:00 a.m. Local Time, Tuesday through Saturday
Major Upgrades	Up to 4 times a year Saturday 10:00 p.m. to Monday 6:00 a.m. Local Time

SAP Signature Management by DocuSign

To the extent maintenance must be performed on the Cloud Service, SAP shall use maintenance windows for planned downtimes applicable to the SAP cloud solution associated with use of the Cloud Service.

SAP SportsOne

	Maintenance Windows
Regular Maintenance Windows	Bi-weekly, Tuesday 6:00 a.m. to Tuesday 8:00 a.m. Local Time Thursdays 6:00 a.m. to Thursday 7:00 a.m. Local Time
Major Upgrades	Once per year, 8 hours

SAP SuccessFactors Business Execution Suite and SAP Learning Hub

	Maintenance Windows
Regular Maintenance Windows	<p>US and Canada data centers: weekly, midnight (Friday-Saturday) to 7:00 a.m. Saturday U.S. Eastern Time and midnight (Saturday-Sunday) to 7:00 a.m. Sunday U.S. Eastern Time;</p> <p>Europe data centers: weekly, midnight (Friday-Saturday) to 7:00 a.m. Saturday GMT and midnight (Saturday-Sunday) to 7:00 a.m. Sunday GMT;</p> <p>Asia Pacific/Australian data center: weekly, midnight (Friday-Saturday) to 7:00 a.m. Saturday AU Eastern Time and midnight (Saturday-Sunday) to 7:00 a.m. Sunday AU Eastern Time; and</p> <p>China data center: weekly, midnight (Friday-Saturday) to 7:00 a.m. Saturday China Standard Time and midnight (Saturday-Sunday) to 7:00 a.m. Sunday China Standard Time.</p>

SAP SuccessFactors Email Encryption

	Maintenance Windows
Regular Maintenance Windows	<p>US and Canada data centers: weekly, midnight (Friday-Saturday) to 7:00 a.m. Saturday U.S. Eastern Time and midnight (Saturday-Sunday) to 7:00 a.m. Sunday U.S. Eastern Time;</p> <p>Europe data centers: weekly, midnight (Friday-Saturday) to 7:00 a.m. Saturday GMT and midnight (Saturday-Sunday) to 7:00 a.m. Sunday GMT;</p> <p>Asia Pacific/Australian data center: weekly, midnight (Friday-Saturday) to 7:00 a.m. Saturday AU Eastern Time and midnight (Saturday-Sunday) to 7:00 a.m. Sunday AU Eastern Time; and</p> <p>China data center: weekly, midnight (Friday-Saturday) to 7:00 a.m. Saturday China Standard Time and midnight (Saturday-Sunday) to 7:00 a.m. Sunday China Standard Time.</p>

SAP Jam

	Maintenance Windows
<p>Regular Maintenance Windows*</p> <p>*In addition to the maintenance windows for the SAP SuccessFactors Business Execution Suite</p>	<p>Weekly, Midnight (Thursday-Friday) to 1:00 a.m. Friday U.S. Eastern Time for the US and Canada data centers;</p> <p>Weekly, 11:00 p.m. Thursday to midnight (Thursday-Friday) Central European Time for the Europe data centers; and</p> <p>Weekly, 7:00 a.m. to 8:00 a.m. Saturday China Standard Time for the China data center.</p>

SAP Jam Communities

	Maintenance Windows
Regular Maintenance Windows	<p>Thursday between 5:00 p.m. and 6:00 p.m. U.S. Eastern Time</p> <p>Midnight (Friday-Saturday) to 7:00 a.m. U.S. Eastern Time</p>

Recruiting Marketing

	Maintenance Windows
Regular Maintenance Windows	<p>Weekly, Fridays from 11:00 p.m. to 3:00 a.m. U.S. Eastern Time and Saturdays from 7:00 a.m. to 10:00 a.m. U.S. Eastern Time</p>

SAP Time and Attendance Management by Workforce Software

	Maintenance Windows
Regular Maintenance Windows	Weekly, Sunday 2:00 a.m. to 6:00 a.m., Local Time

SAP TwoGo

	Maintenance Windows
Regular Maintenance Windows	As required with one (1) day notice to site administrator of Customer.
Major Upgrades	Up to once a month from Friday 10:00 p.m. to Monday 3:00 a.m. Central European Time (CET).

SAP U.S. Benefits Management by Benefitfocus

	Maintenance Windows
Regular Maintenance Windows	Friday 11:00 p.m. to Saturday 7:00 a.m. Eastern U.S. time.

SAP Vehicles Network

	Maintenance Windows
Regular Maintenance Windows	Weekly, Sunday 08:00 am – 10:00 am Local Time.
Major Upgrades	Quarterly, Saturday 10:00 pm to Monday 06:00 am Local Time.

SAP Workforce Performance Builder

	Maintenance Windows
Regular Maintenance Windows	Weekly, Thursday 4:00 p.m. to Thursday 8:00 p.m. Local Time.
Major Upgrades	Up to 4 times per year from Thursday 4:00 p.m. to Friday 6:00 a.m. Local Time.

DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

1. PREAMBLE

1.1 Schedule. This document including Attachment 1, Appendices 1 and 2 ("**Schedule**") shall become an integral part of the Agreement through its reference from the Order Form signed by Customer. This Schedule serves as a written data processing agreement between SAP and each Data Controller providing Personal Data in connection with its use of the Cloud Service. It furthermore defines the applicable technical and organizational measures SAP implements and maintains to protect Personal Data stored in the production system of the Cloud Service.

1.2 Direct Contractual Relationship.

(a) If Customer and its Affiliates are located within the EEA and the processing of Personal Data by SAP is conducted within the EEA or if Customer and its Affiliates are located outside the EEA, this Schedule only applies between SAP and Customer. In this case, Customer is responsible to flow down the terms and conditions set out in this Schedule to its Affiliates.

(b) If Customer and/or its Affiliates are located within the EEA and SAP is located outside the EEA Sections 5.1 and 5.2 of this Schedule apply.

1.3 Form. The conclusion of the Agreement which incorporates this Schedule shall be evidenced upon SAP's receipt of any of the following:

- (a) signed original Order Form,
- (b) signed Order Form in pdf or similar format, or
- (c) accepted Order Form using DocuSign or a similar product used by SAP to receive an Order Form from Customer.

Should Customer require a written original copy of this Schedule or a separately signed electronic copy of the Schedule it shall submit a request to its SAP sales representative.

1.4 Governance. Customer acts as the Data Controller concerning Personal Data of its own Authorized Users as well as on behalf of and in the name of its Affiliates or third parties in their capacity as Data Controllers permitted by Customer to use the Cloud Service. Customer shall serve as a single point of contact for SAP and is solely responsible for the internal coordination, review and submission of instructions or requests of other Data Controllers to SAP. SAP shall be discharged of its obligation to inform or notify a Data Controller when it has provided such information or notice to Customer. SAP is entitled to refuse any requests or instructions provided directly by a Data Controller that is not Customer. Customer warrants that it is entitled to disclose Personal Data to SAP within the Cloud Service as per the Agreement. Customer agrees to hold SAP harmless for claims brought against SAP or its Subprocessors in connection with any breaches of the Customer's Data Protection duties.

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

2. DATA PROCESSING PURPOSES

2.1 Appendix 1. Customer and the respective Data Controllers shall determine the purposes of collecting, processing, and otherwise using Personal Data stored in the Cloud Service. Unless provided otherwise in the Agreement, Appendix 1 of the Schedule shall apply to such data processing.

2.2 Purposes. The purposes for processing Personal Data by SAP and its Subprocessors under this Schedule are limited to:

- (a) Setting up, operating, monitoring and providing the Cloud Service, including the underlying infrastructure (hardware, software, secure data center facilities, connectivity), as a Data Processor or Subprocessor as set forth in the Agreement,
- (b) Providing technical support as a main obligation of SAP under the Agreement,

- (c) Providing Consulting Services as a main obligation of SAP, if and to the extent agreed by the parties,
- (d) Communicating to Authorized Users as clarified in the terms associated with a particular Cloud Service and
- (e) Executing instructions of Customer in accordance with Sections 3.1 and 3.2 below.

3. SAP OBLIGATIONS

3.1 Instructions. SAP shall process Personal Data only in accordance with each Data Controller's instructions submitted by Customer. SAP shall use reasonable commercial efforts to follow and comply with the instructions received from Customer as long as they are legally required and technically feasible and do not require any material modifications to the functionality of the Cloud Service or underlying software. SAP shall notify Customer if SAP considers an instruction submitted by Customer to be in violation of the applicable Data Protection Law. SAP shall not be obligated to perform a comprehensive legal examination. If and to the extent SAP is unable to comply with an instruction it shall promptly notify (email permitted) Customer hereof.

3.2 Instructions based on Data Subject Remedies. SAP may, upon the instruction of Customer and with Customer's necessary cooperation, correct, erase and/or block any Personal Data if and to the extent the functionality of the Cloud Service does not allow Customer, its Data Controllers or Authorized Users to do so. In the event that SAP needs to access any of Customer's systems or Customer's instance of the Cloud Service remotely to execute an instruction or provide technical support, e.g. via application sharing, Customer hereby grants to SAP the permission for such remote access. Further, Customer will name a contact person that – if necessary – can grant to SAP the required access rights.

3.3 Data Secrecy. For processing Personal Data, SAP and its Subprocessors shall only use personnel who are subject to a binding obligation to observe data secrecy or secrecy of telecommunications, to the extent applicable, pursuant to the Data Protection Law. SAP shall itself and shall require that its Subprocessors regularly train individuals to whom they grant access to Personal Data in data security and data privacy.

3.4 Technical and Organizational Measures.

- (a) SAP shall, as a minimum, implement and maintain appropriate technical and organizational measures as described in [Appendix 2](#) of the Schedule.
- (b) Appendix 2 applies to the production system of the Cloud Service to keep Personal Data secure and protect it against unauthorized or unlawful processing and accidental loss, destruction or damage. Non-production environments (e.g. a test instance of the Cloud Service) provide for a lower level of security and SAP recommends that Customer does not store any Personal Data in such non-production environments.
- (c) Since SAP provides the Cloud Service to all customers uniformly via a hosted, web-based application, all appropriate and then current technical and organizational measures apply to SAP's entire customer base hosted out of the same data center and subscribed to the same Cloud Service. Customer understands and agrees that the technical and organizational measures are subject to technical progress, development and improvements for the protection of Personal Data shall automatically apply.

3.5 Verification. SAP shall regularly test the measures described in [Appendix 2](#). If a Data Controller believes that additional measures are required under the applicable Data Protection Law Customer shall submit an instruction according to Section 1.1 above.

3.6 Security Breach Notification. SAP shall promptly inform Customer as soon as it becomes aware of serious disruptions of the processing operations, or any Security Breach in connection with the processing of Personal Data which, in each case, may significantly harm the interest of the Data Subjects concerned.

3.7 Cooperation. At Customer's request and expense, SAP shall reasonably support Customer or other Data Controllers in dealing with requests from individual Data Subjects and/or a supervisory authority with respect to the processing of Personal Data hereunder.

3.8 Deletion. At the end of the Agreement, SAP will delete the Personal Data remaining on servers hosting the Cloud Service unless applicable law or the Agreement requires retention. Retained data is subject to the confidentiality provisions of the Agreement.

4. SUBPROCESSORS

4.1 Permitted Use.

- (a) Customer (also on behalf of its Data Controllers) hereby authorizes SAP (also for the purpose of Clause 11 paragraph 1 of the Standard Contractual Clauses) to engage subcontractors for the processing of Personal Data (each a "**Subprocessor**") (i) to the extent necessary to fulfill its contractual obligations under the Agreement and (ii) 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.
- (b) SAP shall pass on to Subprocessors SAP's obligation as Data Processor (or Subprocessor) vis-à-vis Customer and the respective Data Controllers as set out in this Schedule.
- (c) SAP undertakes to have a selection process by which it evaluates the security, privacy and confidentiality practices of a Subprocessor in regard to data handling on a scheduled basis. Alternatively, the Subprocessor shall possess a security certification that evidences appropriate security measures are in place with regard to the Subprocessor's services to be provided to SAP.
- (d) SAP will inform Customer upon its request by email about the name, address and role of each Subprocessor it uses to provide the Cloud Service.

4.2 New Subprocessors.

- (a) SAP may remove, replace or appoint suitable and reliable further Subprocessors at its own discretion in accordance with this Section 4.2.
- (b) SAP will notify Customer by email in advance (except for Emergency Replacements under Section 4.3) of any changes to the list of Subprocessors, which shall be deemed accepted as long as they comply with and are bound by applicable Data Protection Law or, if a Subprocessor is a Non-EEA Entity, the Standard Contractual Clauses shall apply. If Customer does not object within thirty (30) days after receipt of SAP's notice the new Subprocessor(s) shall be deemed accepted.
- (c) If Customer has a legitimate reason to object to SAP's use of a Subprocessor (e.g. if the Subprocessor is a Non-EEA Entity and Customer needs to complete additional formalities as a Data Controller prior to the use of such Subprocessor) Customer shall notify SAP thereof in writing within thirty days after receipt of SAP's notice. If Customer objects to the use of the Subprocessor concerned SAP shall have the right to cure the objection through one of the following options (to be selected at SAP's sole discretion): (i) SAP will abort its plans to use the Subprocessor with regard to Personal Data; or (ii) SAP will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the Subprocessor with regard to Personal Data; or (iii) SAP may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the Cloud Service that would involve use of the Subprocessor with regard to Personal Data. If none of the above options are reasonably available and the objection has not been cured within thirty(30) days after SAP's receipt of Customer's objection, either party may terminate the affected Cloud Service with reasonable prior written notice.

4.3 "Emergency Replacement" refers to a sudden replacement of a Subprocessor where such change is outside of SAP's reasonable control (such as if the Subprocessor ceases business, abruptly discontinues services to SAP, or breaches its contractual duties owed to SAP). In such

case, SAP will inform Customer of the replacement Subprocessor as soon as possible and the process to formally appoint such Subprocessor pursuant to Section (d) shall be triggered.

5. INTERNATIONAL TRANSFERS AND COUNTRY-SPECIFIC DEVIATIONS

5.1 International Transfer. Personal Data that SAP has received from any Data Controller located in the EEA shall only be exported by SAP or its Subprocessors from the Data Center (whether located in or outside the EEA) to or accessed from a country or territory outside the EEA ("**International Transfer**") if

- (a) the recipient itself or the country or territory in which it operates (i.e. where or from where it processes or accesses Personal Data) has been found to ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data as determined by the European Commission and subject to the scope restrictions of any such determination; or
- (b) the International Transfer to a Non-EEA Entity is in accordance with Section 5.2 below.

5.2 Standard Contractual Clauses. Multi-tier Framework.

- (a) The Standard Contractual Clauses attached to this Schedule ("**Attachment 1**") and Section 4 above apply if the Agreement is concluded between (i) an EEA based Customer or (ii) a Customer with EU based Customer Affiliates and an SAP entity located outside the EEA.
- (b) For any other International Transfer where SAP uses further Non-EEA Entities (appointed under Section 4 above), SAP (represented by SAP SE) has entered into the unchanged version of the Standard Contractual Clauses with each Non-EEA Entity prior to processing Personal Data by means of an International Transfer.
- (c) Customer hereby accedes, and each Data Controller may accede, to the Standard Contractual Clauses set forth in paragraph (b).
- (d) If the preceding direct contract is not available to a Data Controller under mandatory Data Protection Law as determined by SAP and Customer, the Data Controller may enter into the Standard Contractual Clauses furnished by SAP with the relevant Non-EU Entity (represented by SAP SE).
- (e) In the event such direct right to enforce the Standard Contractual Clauses against the relevant Non-EEA Entity does not exist for the Data Controller or is successfully challenged by a Subprocessor, SAP shall enforce such Standard Contractual Clauses against the Subprocessor on behalf of the Data Controller in compliance with this Schedule.
- (f) Nothing in the Agreement shall be construed to prevail over any conflicting Clause of the Standard Contractual Clauses.
- (g) The Standard Contractual Clauses shall be governed by the law of the Member State in which the EEA based Data Exporter is established.

5.3 Country-specific Deviations.

- (a) **Australia.** (i) For the purposes of this Schedule - "**APP**" means the Australian Privacy Principles, from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, and which amended the Privacy Act 1988; "**Data Controller**" means a person who, alone or jointly or in common with other persons, determines the purposes and manner in which any Personal Data are, or are to be, processed; and "**Data Processor**" shall mean any person (other than an employee of the Data Controller) who processes Personal Data on behalf of the Data Controller. (ii) To the extent a Data Controller in Australia or its Authorized Users intend to enter Personal Data into the Cloud Service, Customer agrees to first obtain the consent of each Data Subject to an International Transfer as contemplated under this Schedule if and to the extent required under the applicable data protection law in Australia. Customer hereby confirms and commits that it has received the Personal Data and informed the related Data Subjects regarding the disclosure of the Personal Data in accordance with the APP, and Privacy Act 1988. As such, and on that basis, APP 8.1 is satisfied and shall not otherwise apply by virtue of the "informed

consent" exception under APP 8.2(b) ("**Informed Consent**"). To the extent that Informed Consent may not apply, this Schedule provides the framework for the protection of that Personal Data of those Australian Data Subjects in a way that, overall, is at least substantially similar which the APP's protect that information and SAP agrees to afford to such Personal Data a similar level of protection as set forth in Sections 2, 3 and 6 of this Schedule (by virtue of the "substantially similar law" exception under APP 8.2(a)) ("**Substantially Similar Law**"), and as such, and on that basis, APP 8.1 is satisfied and shall not otherwise apply by virtue of Substantially Similar Law.

- (b) **Austria.** To the extent a Data Controller in Austria or its Authorized Users intend to enter personal data of legal entities (also considered personal data under the Federal Act concerning the Protection of Personal Data (DSG 2000)) into the Cloud Service, Customer agrees to first obtain the consent (in the sense of § 12 para. 3 of the DSG 2000) of such legal entity (Data Subject) before using the Cloud Service, as described herein, for such Data Subject(s). SAP agrees to afford to such personal data a similar level of protection as set forth in Sections 2, 0 and 6 of this Schedule.
- (c) **Russian Federation.** Customer or Customer Affiliates as Data Controllers remain operators of Personal Data of Russian citizens submitted for processing to SAP and are responsible for determining (i) if Customer will be able to comply with applicable Russian privacy law in use of the Cloud Service which involve processing of Russian citizen's Personal Data and (ii) whether the Cloud Service can be used inside or outside the Russian Federation.
- (d) **Singapore.** In accordance with regulation 10(2)(b) of the Personal Data Protection Regulations 2014, unless otherwise stated in the Order Form, the countries to which SAP may transfer Personal Data contained in the Customer Data in the provision of the Cloud Service under the Agreement (as of the effective date of the Order Form signed by Customer) are Australia, Austria, Brazil, Bulgaria, Canada, Chile, China, China/Hong Kong, Czech Republic, France, Germany, Hungary, India, Ireland, Israel, Malaysia, Mexico, the Netherlands, Peru, the Philippines, Poland, the Russian Federation, Singapore, Slovakia, South Africa, South Korea, Spain, Sweden, the United Kingdom, and the United States of America. SAP may add new countries to the above list of countries via the process for notifying Customer of any changes to SAP's list of Subprocessors set forth in Section (d) above, with such notice to include the country in which any new Subprocessor is located. This Section does not necessarily include all countries to which SAP may transfer Customer Data at the direction of Customer or the countries from which Customer, its Authorized Users or Customer's Business Partners may access the Cloud Service.
- (e) **South Korea.** To the extent a Data Controller in Republic of Korea or its Authorized Users intend to enter Personal Data into the Cloud Service, Customer agrees to first obtain the consent of each Data Subject to an International Transfer as contemplated under this Schedule if and to the extent required under the applicable Personal Information Protection Act in Republic of Korea. Customer hereby confirms and commits that it has received the Personal Data and informed the related persons regarding the transfer/process of the Personal Data in accordance with the applicable law.
- (f) **Switzerland.** To the extent a Data Controller in Switzerland or its Authorized Users intend to enter personal data of legal entities (also considered personal data under the Swiss Federal Act on Data Protection) into the Cloud Service, Customer agrees to first obtain the consent (in the sense of Art. 6 para. 2, lit. b. of the Swiss Federal Act on Data Protection) of such legal entity ("**Data Subject**") before using the Cloud Service, as described herein, for such Data Subject(s). SAP agrees to afford to such personal data a similar level of protection as set forth in Sections 2, 0 and 6 of this Schedule.
- (g) **Turkey.** To the extent a Data Controller in Turkey or its Authorized Users intend to enter Personal Data into the Cloud Service, Customer agrees to first obtain the consent of each Data Subject to an International Transfer as contemplated under this Schedule if and to the

extent required under the applicable data protection law in Turkey. Customer hereby confirms and commits that it has received the Personal Data and informed the related persons regarding the transfer/process of the Personal Data in accordance with the applicable law.

- (h) **United States.** Unless SAP and Customer have executed a so called Business Associate agreement for the exchange of protected health information ("**PHI**") as defined in the United States Health Insurance Portability and Accountability Act of 1996, as amended, in relation to the Cloud Service, Customer hereby represents that Customer will not submit PHI to the Cloud Service nor solicit such information from partners or customers as part of use of the Cloud Service.

6. CERTIFICATIONS AND AUDITS

6.1 Certifications and Audit Reports. For the production systems which run the Cloud Service and during the term of the Agreement SAP shall maintain, at its own expense, applicable certifications or audit reports:

- (a) As a minimum, SAP engages an internationally recognized independent third party auditor to review the measures in place in protection of the Cloud Service: (i) Certifications may be based on ISO 27001 or other standards (scope as defined in certificate). (ii) For certain SAP Cloud Services, SAP additionally provides a valid ISAE3402 or SSAE16-SOC 1 Type 2 and/or ISAE3000 or SSAE16-SOC 2 Type 2 report. Upon Customer's request, SAP shall inform Customer about the applicable certifications and audit standards available for the Cloud Service concerned.
- (b) Upon Customer's request, SOC-Audit reports or ISO certifications are available through the third party auditor or SAP, as applicable.

6.2 Customer Audits. Subject to Section 6.4 below and as required under the mandatory Data Protection Law, Customer (or an independent third party auditor on its behalf that is subject to confidentiality obligations consistent with those in the Agreement) may audit SAP's control environment and security practices relevant to Personal Data processed hereunder for Customer in any of the following events:

- (a) SAP has not provided sufficient evidence of its compliance under Section 6.1,
- (b) An event set out in Section **Error! Reference source not found.** above has occurred,
- (c) Customer or another Data Controller has reasonable grounds to suspect that SAP is not in compliance with its obligations under this Schedule,
- (d) A further audit is required by Customer's or another Data Controller's data protection authority or regulator (e.g. in case a law enforcement agency has the right to audit a Data Controller if the Personal Data was processed at the premise of the Data Controller).

6.3 Cooperation. SAP shall reasonably support Customer throughout its verification processes required under the Data Protection Law and provide Customer with the necessary information.

6.4 Audit Restrictions.

- (a) Unless required by mandatory Data Protection Law, an audit pursuant to Section (b) is limited to once in any twelve month period.
- (b) An audit may not exceed three business days.
- (c) Customer shall provide SAP with reasonable prior written notice (at least 60 days unless a data protection authority requires Customer's earlier control under mandatory Data Protection Law).
- (d) Customer and SAP shall mutually agree the scope and determine the agenda of the audit in advance. The audit shall, to the extent possible, rely on certifications and audit reports or other verifications available to confirm SAP's compliance with this Schedule and exclude any repetitive audits.
- (e) Customer shall conduct the audit under reasonable time, place and manner conditions and provide SAP with a copy of the audit report.

- (f) Each party shall bear its own costs for an audit under Section (b) except that Customer shall bear also SAP's costs of SAP's internal resources required to conduct any audit under Section (b)(d) or under mandatory Data Protection Law. SAP's internal costs shall be based on the then-current daily professional service rates as applicable to Customer or, in lack of such agreement, on SAP's price list.
- (g) If an audit determines that SAP has breached its obligations under this Schedule (a "Finding") SAP shall promptly remedy such Finding. It is at SAP's sole discretion to determine which measures are best suitable to ensure compliance under this Schedule.

7. DEFINITIONS

Any capitalized terms used herein, such as Affiliates, Agreement, Customer, Authorized User (sometimes also referred to as User or Named User), Order Form or Cloud Service (sometimes also referred to as Service), shall have the meaning given to them in the Agreement.

- 7.1 "Data Center" means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as published at: <http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html> or notified to Customer or otherwise agreed in an Order Form.
- 7.2 "Data Controller" has the meaning given to this term under the applicable Data Protection Law.
- 7.3 "Data Exporter" as used in the Standard Contractual Clauses means Customer as listed in an Order Form or its Data Controller(s).
- 7.4 "Data Importer" as used in the Standard Contractual Clauses means the applicable Non-EEA Entity.
- 7.5 "Data Processor" has the meaning given to this term under the applicable Data Protection Law.
- 7.6 "Data Protection Law" means the legislation protecting the fundamental rights and freedoms of persons and, in particular, their right to privacy, with regard to the processing of Personal Data under the Agreement. SAP shall comply with additional obligations set out in an Order Form that are required under compelling local data protection laws applicable to SAP as the Data Processor.
- 7.7 "Data Subject" means and identified or identifiable individual or a legal entity (where so defined under the applicable Data Protection Law).
- 7.8 "EEA" means the European Economic Area as well as any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.
- 7.9 "European Subprocessor" means a Subprocessor that is physically processing Personal Data in the EU, Iceland, Liechtenstein, Norway, or Switzerland.
- 7.10 "Non-EEA Entity" means any SAP entity or Subprocessor incorporated outside the EEA, i.e. in a country, which does not provide an adequate level of data protection as determined by the European Commission.
- 7.11 "Personal Data" has the meaning given to that expression in the Data Protection Law and, for the purposes of this Schedule, includes only such personal data entered by Customer or its Authorized Users into or derived from their use of the Cloud Service or supplied to or accessed by SAP or its Subprocessors in order to provide support in accordance with the Agreement. Personal Data is a sub-set of Customer Data and used herein when any Data Protection Law applies.
- 7.12 "SAP" means the SAP entity that is the party to the Order Form that incorporates this Schedule.
- 7.13 "Security Breach" means any acts or omissions by SAP or its Subprocessors that led to an unauthorized disclosure of Personal Data in breach of the measures set forth in [Appendix 2](#) or similar incident for which the Data Controller is legally required to provide notice to the Data Subject or the data protection authority concerned.
- 7.14 "Standard Contractual Clauses" or sometimes also referred to the "EU Model Clauses" means 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), or any subsequent version thereof released by the Commission (which shall automatically apply), including Appendices 1 and 2 attached hereto.

7.15 "Subprocessor" as used in the Standard Contractual Clauses and this Schedule means the SAP Affiliates and third party subprocessors engaged by SAP or SAP's Affiliates in accordance with Section 4.

8. EU ACCESS (OPTION)

8.1 Eligible Cloud Service. In deviation of Section 5.1 of this Schedule, SAP agrees to provide EU Access for the Cloud Service if and to the extent agreed on the Order Form. Customer understands that EU Access is provided only for EU Access eligible services, as determined by SAP from time to time, that are hosted by SAP in the EU.

8.2 Data Center Location. Upon the Order Form Effective Date and in deviation of any conflicting provision in the Order Form, the Data Centers used to host Personal Data in the ordered Cloud Service are located in the territory of the EEA or Switzerland. SAP undertakes not to migrate the Customer instance to a Data Center outside the territory of the EEA or Switzerland without Customer's prior written consent (email permitted). If SAP plans to migrate the Customer instance to a data center within the EEA or to Switzerland SAP shall notify Customer in writing (email permitted) thereof no later than thirty days before the planned migration.

8.3 EU Access. Customer has requested and SAP has agreed to refrain from using Subprocessors other than European Subprocessors in providing support of the production systems of the Cloud Service to the extent such support may require access to Personal Data whether or not such access occurs.

8.4 Exclusion. The following Personal Data is not subject to EU Access:

- (a) Contact details of the sender of a support and/or incident ticket, notice or message when filing a support and/or incident ticket
- (b) Any other Personal Data submitted by Customer when filing a support and/or incident ticket. Customer may choose not to transmit such Personal Data when filing a support and/or incident ticket. If such data is necessary for the incident management process, Customer may choose to anonymize such Personal Data before any transmission of the incident message to SAP
- (c) Personal Data in non-production systems.

Personal Data that is not subject to EU Access shall only be transferred or accessed by SAP or its Subprocessors in accordance with Section 5.

-- REMAINDER OF PAGE INTENTIONALLY LEFT BLANK --

Attachment 1
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)¹

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

Customer and/or Customer Affiliates based in the EU in the sense of Section 1.2 (b) of the DATA PROCESSING AGREEMENT (in the Clauses hereinafter referred to as the '**data exporter**')

and

SAP SE as representative for Non-EEA Entities in the sense of Section 5.2 of the DATA PROCESSING AGREEMENT (in the Clauses hereinafter referred to as the '**data importer**')

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) 'the data exporter' means the controller who transfers the personal data;
- (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

¹ Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the

processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

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

Clause 10

Variation of the contract

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

Clause 11
Sub-processing

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

Clause 12
Obligation after the termination of personal data-processing services

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

APPENDIX 1 TO DATA PROCESSING AGREEMENT AND STANDARD CONTRACTUAL CLAUSES

The parties may provide further details in an Order Form or the Supplement, if required, or adjusted in the description below by Customer.

Data Exporter

The Data Exporter subscribed to a SAP Cloud Service which allow Authorized Users to enter, amend, use, delete or otherwise process Personal Data as contemplated under the Agreement.

Data Importer

SAP and its Subprocessors provide the Cloud Service which includes the following Support: SAP Affiliates around the world support the global SAP Cloud Service data centers remotely from SAP facilities, e.g. in St. Leon/Rot (Germany), India and other locations where SAP employs personnel in the Operations/Cloud Delivery function. Support includes but is not limited to:

- Monitoring the Cloud Service and underlying infrastructure
- Backup & restore Customer Data stored in the Cloud Service
- Release and development of patches, new updates and upgrades to the Cloud Service and underlying infrastructure
- Troubleshooting for servers, storage, network equipment
- Database monitoring, troubleshooting, day-to-day database administration activities incl. production database sizing, index creation, performance tuning, patch management. Standby database management and projects related to database functions
- Security monitoring, network-based intrusion detection support, conducting penetration tests

SAP Affiliates provide also support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users (incident): SAP answers phones and performs basic troubleshooting and routes and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data subjects

The Personal Data transferred concern the following categories of data subjects:

Unless provided otherwise by Data Exporter, Data Subjects may include employees, contractors, business partners or other individuals whose Personal Data is stored in the Cloud Service.

Categories of data

The Personal Data transferred concern the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer's data fields can be configured as part of the implementation of the Cloud Service or as otherwise permitted in the Cloud Service. The Personal Data transferred usually concern (a subset of) the following categories of data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data which Authorized Users enter into the Cloud Service including bank account data, credit or debit card data.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data: As set out in the Order Form, if any.

Processing operations

The Personal Data transferred will be subject to the following basic processing activities:

- use of Personal Data to provide the Cloud Service (including Operational and Technical Support)
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any patch, update, upgrade / new releases to the Cloud Service
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer, if required

APPENDIX 2 TO DATA PROCESSING AGREEMENT AND STANDARD CONTRACTUAL CLAUSES

1. PREAMBLE

- 1.1 Deviations.** Some Cloud Services are subject to different support terms, as set forth in the respective Supplement or Order Form.
- 1.2 Scope.** In all other cases, the description of the technical and organizational security measures set out in Section 2 below implemented by the Data Importer for Personal Data stored in the production system of the Cloud Service (in accordance with Clauses 4(d) and 5(c) of the Standard Contractual Clauses) shall apply.

2. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define the current security measures established by SAP.

- 2.1 Physical Access Control.** Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located which process and/or use Personal Data.

Measures:

All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To ensure proper functionality, physical security equipment (e.g. motion sensors, cameras, etc.) are maintained on a regular basis. In detail, the following physical security measures are implemented at all Data Centers:

- (a) SAP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- (b) In general, buildings are secured through access control systems (smart card access system).
- (c) As a minimum requirement, the outermost shell of the building must be fitted with a certified key system including modern, active key management.
- (d) Depending on the security classification, buildings, individual areas and surrounding premises are further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- (e) Access rights will be granted to authorized persons on an individual basis according to the System and Data Access Control measures set out below. This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel. SAP and all third party Data Center providers are logging the names and times of persons entering the private areas of SAP within the Data Centers.
- (f) SAP employees and external personnel must wear their ID cards at all SAP locations.

- 2.2 System Access Control.** Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

- (a) Multiple authorization levels are used to grant access to sensitive systems including those storing and processing Personal Data. Processes are in place to ensure that only authorized users have the appropriate authorization to add, delete, or modify users.
- (b) All users access SAP's systems with a unique identifier (user ID).
- (c) 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 changes roles or leaves the company, its access rights are revoked.
- (d) SAP has established a password policy that prohibits the sharing of passwords, governs what

to do if a password is disclosed, requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In case of domain passwords, the system forces a password change every six months complying with the requirements for complex passwords. Each computer has a password-protected screensaver.

- (e) Remote access to the Cloud Service delivery environment requires at least strong authentication mechanisms (for instance a combination of a password and an additional security feature). Passwords with a minimum length of fifteen (15) characters must be used for administrative accounts and service accounts of security-critical IT systems. New passwords must be different from an Authorized User's last five (5) passwords. The company network is protected from the public network by firewalls.
- (f) SAP uses up-to-date antivirus software at access points to the company network (for e-mail accounts) and on all file servers and all workstations.
- (g) A security patch management is implemented to ensure deployment of relevant security updates.
- (h) Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

2.3 Data Access Control. Persons entitled to use data processing systems shall gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

- (a) 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 SAP security policies and standards.
- (b) All production servers of any SAP Cloud Service are operated in the relevant Data Centers/server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on the IT systems.
- (c) SAP does not allow the installation of personal software or other software not approved by SAP to systems being used for any Cloud Service.
- (d) A SAP security standard governs how data and data carriers are deleted or destroyed.

2.4 Data Transmission Control. Personal Data must not be read, copied, modified or removed without authorization during transfer.

Measures:

- (a) Where data carriers are physically transported, adequate measures are implemented at SAP to ensure the agreed service levels (for example, encryption, and lead-lined containers).
- (b) Personal Data transfer over SAP internal networks are protected as any other confidential data according to SAP Security Policy.
- (c) When the data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed in the Agreement. This applies to both physical and network based data transfer. In any case the Customer assumes responsibility for any data transfer from SAP's Point of Demarcation (e.g. outgoing firewall of the SAP Data Center which hosts the Cloud Service).

2.5 Data Input Control. It shall be possible to retrospectively examine and establish whether and by whom at SAP Personal Data have been entered, modified or removed from data processing systems used to provide the Cloud Service.

Measures:

SAP only allows authorized persons to access Personal Data as required in the course of their work. SAP implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its Subprocessors to the greatest extent supported by the Cloud Service.

2.6 Job Control. Personal Data being processed on commission shall be processed solely in accordance with the Agreement and related instructions of the Customer.

Measures:

- (a) SAP uses controls and processes to ensure compliance with contracts between SAP and its customers, Subprocessors or other service providers.
- (b) As part of the SAP Security Policy, Customer Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- (c) All SAP employees and contractual partners are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

2.7 Availability Control. Personal Data shall be protected against accidental or unauthorized destruction or loss.

Measures:

- (a) SAP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
- (b) SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.
- (c) SAP has defined contingency plans as well as business and disaster recovery strategies for Cloud Services.
- (d) Emergency processes and systems are regularly tested.

2.8 Data Separation Control. Personal Data collected for different purposes can be processed separately.

Measures:

- (a) 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 customer.
- (b) SAP maintains dedicated instances (with logical or physical separation) for each Customer.
- (c) Customers (including their Affiliates) have access only to own Customer instance(s).

2.9 Data Integrity Control. Ensures that Personal Data will remain intact, complete and current during processing activities:

Measures:

SAP has implemented a defense strategy in several layers as a protection against unauthorized modifications. This refers to controls as stated in the control and measure sections as described above.

In particular:

- (a) Firewalls;

- (b) Security Monitoring Center;
- (c) Antivirus software;
- (d) Backup and recovery;
- (e) External and internal penetration testing;
- (f) Regular external audits to prove security measures.

-- REMAINDER OF PAGE INTENTIONALLY LEFT BLANK --

GENERAL TERMS AND CONDITIONS FOR SAP CLOUD SERVICES ("GTC")

1. DEFINITIONS

Commonly used capitalized terms are defined in the Glossary at the end of the document.

2. USAGE RIGHTS AND RESTRICTIONS

2.1 Grant of Rights.

SAP grants to Customer a non-exclusive, non-transferable and world-wide right to use the Cloud Service (including its implementation and configuration), Cloud Materials and Documentation solely for Customer's and its Affiliates' internal business operations. Permitted uses and restrictions of the Cloud Service also apply to Cloud Materials and Documentation.

2.2 Authorized Users.

Customer may permit Authorized Users to use the Cloud Service. Usage is limited to the Usage Metrics and volumes stated in the Order Form. Access credentials for the Cloud Service may not be used by more than one individual, but may be transferred from one individual to another if the original user is no longer permitted to use the Cloud Service. Customer is responsible for breaches of the Agreement caused by Authorized Users.

2.3 Acceptable Use Policy.

With respect to the Cloud Service, Customer will not:

- (a) disassemble, decompile, reverse-engineer, copy, translate or make derivative works,
- (b) transmit any content or data that is unlawful or infringes any intellectual property rights, or
- (c) circumvent or endanger its operation or security.

2.4 Verification of Use.

Customer will monitor its own use of the Cloud Service and report any use in excess of the Usage Metrics and volume. SAP may monitor use to verify compliance with Usage Metrics, volume and the Agreement.

2.5 Suspension of Cloud Service.

SAP may suspend use of the Cloud Service if continued use may result in material harm to the Cloud Service or its users. SAP will promptly notify Customer of the suspension. SAP will limit the suspension in time and scope as reasonably possible under the circumstances.

2.6 Third Party Web Services.

The Cloud Service may include integrations with web services made available by third parties (other than SAP SE or its Affiliates) that are accessed through the Cloud Service and subject to terms and conditions with those third parties. These third party web services are not part of the Cloud Service and the Agreement does not apply to them.

3. SAP RESPONSIBILITIES

3.1 Provisioning.

SAP provides access to the Cloud Service as described in the Agreement.

3.2 Support.

SAP provides support for the Cloud Service as referenced in the Order Form.

3.3 Security.

SAP uses reasonable security technologies in providing the Cloud Service. As a data processor, SAP will implement technical and organizational measures referenced in the Order Form to secure personal data processed in the Cloud Service in accordance with applicable data protection law.

3.4 Modifications.

- (a) The Cloud Service and SAP Policies may be modified by SAP. SAP will inform Customer of modifications by email, the support portal, release notes, Documentation or the Cloud Service. The information will be delivered by email if the modification is not solely an

enhancement. Modifications may include optional new features for the Cloud Service, which Customer may use subject to the then-current Supplement.

- (b) If Customer establishes that a modification is not solely an enhancement and materially reduces the Cloud Service, Customer may terminate its subscriptions to the affected Cloud Service by providing written notice to SAP within thirty days after receipt of SAP's informational notice.

3.5 Analyses.

SAP, SAP SE or SAP Affiliates may use anonymous information relating to use of the Cloud Service and Consulting Services to prepare analyses. Analyses do not contain Customer Confidential Information. Examples of analyses include: optimizing resources and support, research and development, verification of security and data integrity, internal demand planning, industry developments and anonymous benchmarking with other Customers. SAP may provide non-anonymous benchmarking services with Customer's prior written consent.

4. CUSTOMER AND PERSONAL DATA

4.1 Customer Data.

Customer is responsible for the Customer Data and entering it into the Cloud Service. Customer grants to SAP (including SAP SE, its Affiliates and subcontractors) a nonexclusive right to process Customer Data (including personal data) solely to provide and support the Cloud Service.

4.2 Personal Data.

Customer will collect and maintain all personal data contained in the Customer Data in compliance with applicable data privacy and protection laws.

4.3 Security.

Customer will maintain reasonable security standards for its Authorized Users' use of the Cloud Service.

4.4 Access to Customer Data.

- (a) During the Subscription Term, Customer can access its Customer Data at any time. Customer may export and retrieve its Customer Data in a standard format. Export and retrieval may be subject to technical limitations, in which case SAP and Customer will find a reasonable method to allow Customer access to Customer Data.
- (b) Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Customer Data from the Cloud Service.
- (c) At the end of the Agreement, SAP will delete the Customer Data remaining on servers hosting the Cloud Service unless applicable law requires retention. Retained data is subject to the confidentiality provisions of the Agreement.
- (d) In the event of third party legal proceedings relating to the Customer Data, SAP will cooperate with Customer and comply with applicable law (both at Customer's expense) with respect to handling of the Customer Data.

5. FEES AND TAXES

5.1 Fees and Payment.

Customer will pay fees as stated in the Order Form. After prior written notice, SAP may suspend Customer's use of the Cloud Service until payment is made. Customer cannot withhold, reduce or set-off fees owed nor reduce Usage Metrics during the Subscription Term. All Order Forms are non-cancellable and fees non-refundable.

5.2 Taxes.

Fees and other charges imposed under an Order Form will not include taxes, all of which will be for Customer's account. Customer is responsible for all taxes, other than SAP's income and payroll taxes. Customer must provide to SAP any direct pay permits or valid tax-exempt certificates prior to signing an Order Form. If SAP is required to pay taxes (other than its income and payroll taxes), Customer will reimburse SAP for those amounts and indemnify SAP for any taxes and related costs paid or payable by SAP attributable to those taxes.

6. TERM AND TERMINATION

6.1 Term.

The Subscription Term is as stated in the Order Form.

6.2 Termination.

A party may terminate the Agreement:

- (a) upon thirty days written notice of the other party's material breach unless the breach is cured during that thirty day period,
- (b) as permitted under Sections 3.4(b), 7.2(b), 7.4(c), or 8.1(c) (with termination effective thirty days after receipt of notice in each of these cases), or
- (c) immediately if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors, or otherwise materially breaches Sections 11 or 12.6.

6.3 Refund and Payments.

For termination by Customer or an 8.1(c) termination, Customer will be entitled to:

- (a) a pro-rata refund in the amount of the unused portion of prepaid fees for the terminated subscription calculated as of the effective date of termination, and
- (b) a release from the obligation to pay fees due for periods after the effective date of termination.

6.4 Effect of Expiration or Termination.

Upon the effective date of expiration or termination of the Agreement:

- (a) Customer's right to use the Cloud Service and all SAP Confidential Information will end,
- (b) Confidential Information of the disclosing party will be returned or destroyed as required by the Agreement, and
- (c) termination or expiration of the Agreement does not affect other agreements between the parties.

6.5 Survival.

Sections 1, 5, 6.3, 6.4, 6.5, 8, 9, 10, 11, and 12 will survive the expiration or termination of the Agreement.

7. WARRANTIES

7.1 Compliance with Law.

Each party warrants its current and continuing compliance with all laws and regulations applicable to it in connection with:

- (a) in the case of SAP, the operation of SAP's business as it relates to the Cloud Service, and
- (b) in the case of Customer, the Customer Data and Customer's use of the Cloud Service.

7.2 Good Industry Practices.

SAP warrants that it will provide the Cloud Service:

- (a) in substantial conformance with the Documentation; and
- (b) with the degree of skill and care reasonably expected from a skilled and experienced global supplier of services substantially similar to the nature and complexity of the Cloud Service.

7.3 Remedy.

Customer's sole and exclusive remedies and SAP's entire liability for breach of the warranty under Section 7.2 will be:

- (a) the re-performance of the deficient Cloud Service, and
- (b) if SAP fails to re-perform, Customer may terminate its subscription for the affected Cloud Service. Any termination must occur within three months of SAP's failure to re-perform.

7.4 System Availability.

- (a) SAP warrants to maintain an average monthly system availability for the production system of the Cloud Service as defined in the applicable service level agreement or Supplement ("SLA").
- (b) Customer's sole and exclusive remedy for SAP's breach of the SLA is the issuance of a credit in the amount described in the SLA. Customer will follow SAP's posted credit claim procedure. When the validity of the service credit is confirmed by SAP in writing (email permitted), Customer may apply the credit to a future invoice for the Cloud Service or request a refund for the amount of the credit if no future invoice is due.
- (c) In the event SAP fails to meet the SLA (i) for four consecutive months, or (ii) for five or more months during any twelve months period, or (iii) at a system availability level of least 95% for one calendar month, Customer may terminate its subscriptions for the affected Cloud Service by providing SAP with written notice within thirty days after the failure.

7.5 Warranty Exclusions.

The warranties in Sections 7.2 and 7.4 will not apply if:

- (a) the Cloud Service is not used in accordance with the Agreement or Documentation,
- (b) any non-conformity is caused by Customer, or by any product or service not provided by SAP, or
- (c) the Cloud Service was provided for no fee.

7.6 Disclaimer.

Except as expressly provided in the Agreement, neither SAP nor its subcontractors 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 or integration with any products or services provided under the Agreement, or that the operation of any products or services will be secure, uninterrupted or error free. Customer agrees that it is not relying on delivery of future functionality, public comments or advertising of SAP or product roadmaps in obtaining subscriptions for any Cloud Service.

8. THIRD PARTY CLAIMS

8.1 Claims Brought Against Customer.

- (a) SAP will defend Customer against claims brought against Customer and its Affiliates by any third party alleging that Customer's and its Affiliates' use of the Cloud Service infringes or misappropriates a patent claim, copyright, or trade secret right. SAP will indemnify Customer against all damages finally awarded against Customer (or the amount of any settlement SAP enters into) with respect to these claims.
- (b) SAP's obligations under Section 8.1 will not apply if the claim results from (i) Customer's breach of Sections 2, (ii) use of the Cloud Service in conjunction with any product or service not provided by SAP, or (iii) use of the Cloud Service provided for no fee.
- (c) In the event a claim is made or likely to be made, SAP may (i) procure for Customer the right to continue using the Cloud Service under the terms of the Agreement, or (ii) replace or modify the Cloud Service to be non-infringing without material decrease in functionality. If these options are not reasonably available, SAP or Customer may terminate Customer's subscription to the affected Cloud Service upon written notice to the other.

8.2 Claims Brought Against SAP.

Customer will defend SAP against claims brought against SAP, SAP SE, its Affiliates and subcontractors by any third party related to Customer Data.

Customer will indemnify SAP against all damages finally awarded against SAP, SAP SE, its Affiliates and subcontractors (or the amount of any settlement Customer enters into) with respect to these claims.

8.3 Third Party Claim Procedure.

- (a) The party against whom a third party claim is brought will timely notify the other party in writing of any claim, reasonably cooperate in the defense and may appear (at its own expense) through counsel reasonably acceptable to the party providing the defense.
- (b) The party that is obligated to defend a claim will have the right to fully control the defense.
- (c) Any settlement of a claim will not include a financial or specific performance obligation on, or admission of liability by, the party against whom the claim is brought.

8.4 Exclusive Remedy.

The provisions of Section 8 state the sole, exclusive, and entire liability of the parties, their Affiliates, Business Partners and subcontractors to the other party, and is the other party's sole remedy, with respect to covered third party claims and to the infringement or misappropriation of third party intellectual property rights.

9. LIMITATION OF LIABILITY

9.1 Unlimited Liability.

Neither party will exclude or limit its liability for damages resulting from:

- (a) the parties' obligations under Section 8.1(a) and 8.2,
- (b) unauthorized use or disclosure of Confidential Information,
- (c) either party's breach of its data protection and security obligations that result in an unauthorized use or disclosure of personal data,
- (d) death or bodily injury arising from either party's gross negligence or willful misconduct, or
- (e) any failure by Customer to pay any fees due under the Agreement.

9.2 Liability Cap.

Subject to Sections 9.1 and 9.3, the maximum aggregate liability of either party (or its respective Affiliates or SAP's subcontractors) to the other or any other person or entity for all events (or series of connected events) arising in any twelve month period will not exceed the annual subscription fees paid for the applicable Cloud Service directly causing the damage for that twelve month period. Any "twelve month period" commences on the Subscription Term start date or any of its yearly anniversaries.

9.3 Exclusion of Damages.

Subject to Section 9.1:

- (a) neither party (nor its respective Affiliates or SAP's subcontractors) will be liable to the other party for any special, incidental, consequential, or indirect damages, loss of good will or business profits, work stoppage or for exemplary or punitive damages, and
- (b) SAP will not be liable for any damages caused by any Cloud Service provided for no fee.

9.4 Risk Allocation.

The Agreement allocates the risks between SAP and Customer. The fees for the Cloud Service and Consulting Services reflect this allocation of risk and limitations of liability.

10. INTELLECTUAL PROPERTY RIGHTS

10.1 SAP Ownership.

SAP, SAP SE, their Affiliates or licensors own all intellectual property rights in and related to the Cloud Service, Cloud Materials, Documentation, Consulting Services, design contributions, related knowledge or processes, and any derivative works of them. All rights not expressly granted to Customer are reserved to SAP, SAP SE and its licensors.

10.2 Customer Ownership.

Customer retains all rights in and related to the Customer Data.

10.3 Non-Assertion of Rights.

Customer covenants, on behalf of itself and its successors and assigns, not to assert against SAP, SAP SE, their Affiliates or licensors, any rights, or any claims of any rights, in any Cloud Service, Cloud Materials, Documentation, or Consulting Services.

11. CONFIDENTIALITY

11.1 Use of Confidential Information.

- (a) Unless deemed as a public record pursuant to Chapter 119, Florida Statutes, the receiving party will protect all Confidential Information of the disclosing party as strictly confidential to the same extent it protects its own Confidential Information, and not less than a reasonable standard of care. Receiving party will not disclose any Confidential Information of the disclosing party to any person other than its personnel, representatives or Authorized Users whose access is necessary to enable it to exercise its rights or perform its obligations under the Agreement and who are under obligations of confidentiality substantially similar to those in Section 11. Customer will not disclose the Agreement or the pricing to any third party.
- (b) Confidential Information of either party disclosed prior to execution of the Agreement will be subject to Section 11.
- (c) In the event of legal proceedings relating to the Confidential Information, the receiving party will cooperate with the disclosing party and comply with applicable law (all at disclosing party's expense) with respect to handling of the Confidential Information.
- (d) Notwithstanding any terms and conditions to the contrary, disclosure of any confidential information received by Customer will be governed by the provisions of the Florida Public Records Act, Chapter 119, Florida Statutes.

11.2 Exceptions.

The restrictions on use or disclosure of Confidential Information will not apply to any Confidential Information that:

- (a) is independently developed by the receiving party without reference to the disclosing party's Confidential Information,
- (b) is generally available to the public without breach of the Agreement by the receiving party,
- (c) at the time of disclosure, was known to the receiving party free of confidentiality restrictions, or
- (d) the disclosing party agrees in writing is free of confidentiality restrictions.

11.3 Publicity.

Except as required by Customer under the Florida Open Meetings Law and/or the Florida Sunshine Law, neither party will use the name of the other party in publicity activities without the prior written consent of the other, except that Customer agrees that SAP may use Customer's name in customer listings or quarterly calls with its investors or, at times mutually agreeable to the parties, as part of SAP's marketing efforts (including reference calls and stories, press testimonials, site visits, SAPPHIRE participation). Customer agrees that SAP may share information on Customer with its Affiliates for marketing and other business purposes and that it has secured appropriate authorizations to share Customer employee contact information with SAP.

12. MISCELLANEOUS

12.1 Severability.

If any provision of the Agreement is held to be invalid or unenforceable, the invalidity or unenforceability will not affect the other provisions of the Agreement.

12.2 No Waiver.

A waiver of any breach of the Agreement is not deemed a waiver of any other breach.

12.3 Electronic Signature.

Electronic signatures that comply with applicable law are deemed original signatures. Upon Customer's request, SAP will execute agreed upon documentation with written signature.

12.4 Regulatory Matters.

SAP Confidential Information is subject to export control laws of various countries, including the laws of the United States and Germany. Customer will not submit SAP Confidential Information to any government agency for licensing consideration or other regulatory approval, and will not export SAP Confidential Information to countries, persons or entities if prohibited by export laws.

12.5 Notices.

All notices will be in writing and given when delivered to the address set forth in an Order Form with copy to the legal department. Notices by SAP relating to the operation or support of the Cloud Service and those under Sections 3.4 and 5.1 may be in the form of an electronic notice to Customer's authorized representative or administrator identified in the Order Form.

12.6 Assignment.

Without SAP's prior written consent, Customer may not assign or transfer the Agreement (or any of its rights or obligations) to any party. SAP may assign the Agreement to SAP SE or any of its Affiliates, subject to Customer's prior written consent, not to be unreasonably withheld; provided however that SAP may assign the Agreement to its parent corporation without Customer consent.

12.7 Subcontracting.

SAP may subcontract parts of the Cloud Service or Consulting Services to third parties. SAP is responsible for breaches of the Agreement caused by its subcontractors.

12.8 Relationship of the Parties.

The parties are independent contractors, and no partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties is created by the Agreement.

12.9 Force Majeure.

Any delay in performance (other than for the payment of amounts due) caused by conditions beyond the reasonable control of the performing party is not a breach of the Agreement. The time for performance will be extended for a period equal to the duration of the conditions preventing performance.

12.10 Governing Law.

The Agreement and any claims relating to its subject matter will be governed by and construed under the laws of the State of Florida, without reference to its conflicts of law principles. All disputes will be subject to the exclusive jurisdiction of the courts located in the State of Florida. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act (where enacted) will not apply to the Agreement. Either party must initiate a cause of action for any claim(s) relating to the Agreement and its subject matter within one year from the date when the party knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

12.11 Entire Agreement.

The Agreement constitutes the complete and exclusive statement of the agreement between SAP and Customer in connection with the parties' business relationship related to the subject matter of the Agreement. All previous representations, discussions, and writings (including any confidentiality agreements) are merged in and superseded by the applicable Agreement and the parties disclaim any reliance on them. An Agreement may be modified solely in writing signed by both parties, except as permitted under Section 3.4. An Agreement will prevail over terms and conditions of any Customer-issued purchase order, which will have no force and effect, even if SAP accepts or does not otherwise reject the purchase order.

Glossary

- 1.1 "Affiliate"** of a party means any legal entity in which a party, directly or indirectly, holds more than fifty percent (50%) of the entity's shares or voting rights. Any legal entity will be considered an Affiliate as long as that interest is maintained.
- 1.2 "Agreement"** means an Order Form and documents incorporated into an Order Form.
- 1.3 "Authorized User"** means any individual to whom Customer grants access credentials to use the Cloud Service that is an employee, agent, contractor or representative of
- (a) Customer,
 - (b) Customer's Affiliates, and/or
 - (c) Customer's and Customer's Affiliates' Business Partners.
- 1.4 "Business Partner"** means a legal entity that requires use of a Cloud Service in connection with Customer's and its Affiliates' internal business operations. These may include customers, distributors, service providers and/or suppliers of Customer.
- 1.5 "Cloud Service"** means any distinct, subscription-based, hosted, supported and operated on-demand solution provided by SAP under an Order Form.
- 1.6 "Cloud Materials"** mean any materials provided or developed by SAP (independently or with Customer's cooperation) in the course of performance under the Agreement, including in the delivery of any support or Consulting Services to Customer. Cloud Materials do not include the Customer Data, Customer Confidential Information or the Cloud Service.
- 1.7 "Confidential Information"** means
- (a) with respect to Customer: (i) the Customer Data, (ii) Customer marketing and business requirements, (iii) Customer implementation plans, and/or (iv) Customer financial information, and
 - (b) with respect to SAP: (i) the Cloud Service, Documentation, Cloud Materials and analyses under Section 3.5, and (ii) information regarding SAP research and development, product offerings, pricing and availability.
 - (c) Confidential Information of either SAP or Customer also includes information which the disclosing party protects against unrestricted disclosure to others that (i) the disclosing party or its representatives designates as confidential at the time of disclosure, or (ii) should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding its disclosure.
- 1.8 "Consulting Services"** means professional services, such as implementation, configuration, custom development and training, performed by SAP's employees or subcontractors as described in any Order Form and which are governed by the Supplement for Consulting Services or similar agreement.
- 1.9 "Customer Data"** means any content, materials, data and information that Authorized Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer-specific reports). Customer Data and its derivatives will not include SAP's Confidential Information.
- 1.10 "Documentation"** means SAP's then-current technical and functional documentation as well as any roles and responsibilities descriptions, if applicable, for the Cloud Service which is made available to Customer with the Cloud Service.
- 1.11 "Order Form"** means the ordering document for a Cloud Service that references the GTC.
- 1.12 "SAP SE"** means SAP SE, the parent company of SAP.
- 1.13 "SAP Policies"** means the operational guidelines and policies applied by SAP to provide and support the Cloud Service as incorporated in an Order Form.
- 1.14 "Subscription Term"** means the term of a Cloud Service subscription identified in the applicable Order Form, including all renewals.
- 1.15 "Supplement"** means the supplemental terms and conditions that apply to the Cloud Service and that are incorporated in an Order Form.
- 1.16 "Usage Metric"** means the standard of measurement for determining the permitted use and calculating the fees due for a Cloud Service as set forth in an Order Form.