Order Form for SAP
Cloud Services
SAP Reference No. 3061788005

Between

SAP (UK) Limited
Clockhouse Place, Bedfont Road
Feltham, Middlesex
TW14 8HD
(Company Number: 2152073)
("SAP")

and **HMRC (Her Majesty's Revenue & Customs)**
100 Parliament Street, London, SW1A 2BQ, LO, United Kingdom Greater London
("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) listed in this Order Form and is effective on the date signed by Customer.

Offer Expiration Date: 22.12.2021

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"**:

Agreement	Location
Order Form	
Schedule A of this Order Form: Cloud Service Supplemental Terms and Conditions ("**Supplement**")	Attached as Appendix 1 of this Order Form
Schedule B of this Order Form: Support Policy for SAP Cloud Services	Attached as Appendix 2 of this Order Form
Schedule C of this Order Form: Service Level Agreement for SAP Cloud Services ("**SLA**")	Attached as Appendix 3 of this Order Form
Schedule D of this Order Form: Data Processing Agreement for SAP Cloud Services enGB.v.7-2020a ("DPA") Schedule D will serve as a commissioned written data processing agreement.	Attached as Appendix 4 of this Order Form

[redacted]	[redacted]
Schedule F of this Order Form: General Terms and Conditions for SAP Cloud Services ("**GTC**")	Attached as Appendix 6 of this Order Form

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.

From 01.01.2022 To 31.12.2024

SAP Cloud Service	Usage Metric	Usage Metric Limitation **	Annual Fee	Product Start Date	Product End Date	Total Fee in GBP
SAP Ariba Supplier Info/Performance Mgt.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
SAP Ariba Commerce Automation Membership	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
SAP Ariba Buying & Invoicing	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Ariba Network, buyer-paid supplier fees	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
SAP Sig Mgmt by DocuSign, premium spend	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
SAP Ariba Strategic Sourcing Suite	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total Net Fee (*)						4,626,561.96
Period From 01.01.2022 To 31.12.2022						[redacted]
Period From 01.01.2023 To 31.12.2023						[redacted]
Period From 01.01.2024 To 31.12.2024						[redacted]
Total Net Fee (*)						4,626,561.96

(*) plus applicable taxes

(**) Usage Metric Limitations stated above represent the maximum annual quantity of Usage Metrics over a 12-month period.

(***) [redacted]

(****) [redacted]

2.2. **Subscription Term**.

2.2.1. Customer's initial Subscription Term will begin on 1st January 2022 and will be effective until 31st December 2024, unless Customer is otherwise notified by SAP's provisioning team.

2.2.2. SAP and Customer may agree to renew the Subscription Term at least 60 days' prior to the end of the current Subscription Term.

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 Net Price Per Unit Per Annum as set out in Table 1 of this Order Form.

2.4. **Price Protection**

At any time during the initial Subscription Term, Customer may purchase additional Usage Metrics of the Cloud Service(s) listed in this Order Form for the remainder of the initial Subscription Term, by signing an amendment to this Order Form and paying additional fees which shall be charged at the same price per unit as set forth herein.

3. PAYMENT AND INVOICES

3.1. Fees and Invoicing.

Unless the Supplement states otherwise, fees for the Cloud Service(s) will be invoiced by SAP and paid by Customer yearly in advance. 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 for Excess Use or as described below, 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. Customer will reimburse SAP for all pre-approved (by Customer) and appropriately documented travel and related expenses incurred by SAP in performing any support for the Cloud Service.

3.2. Fee Increases.

SAP may increase fees for the Cloud Services at the beginning of each renewal Subscription Term. This increase will not exceed [redacted]. Not raising fees is not a waiver of SAP's right to do so. SAP may increase fees if Customer elects to reduce any Cloud Service, Usage Metrics or volume for any renewal Subscription Term. This section does not apply to CPEA Cloud Services or Pay-As-You-Go Cloud Services.

3.3. Payment.

Customer will pay to SAP all fees due within 30 days of date of invoice. Unpaid fees will accrue interest at the [redacted], but not to exceed 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.

4. AUTHORIZED ADMINISTRATORS

Customer confirms the names assigned to the authorized roles are accurate and that the contacts below have been informed of the responsibility. Inaccuracy can result in delays outside of SAP control.

Main Contact:

[redacted]

The Main Contact is the Customer contact for onboarding, who receives the confirmation that the order has been processed (which includes the confirmed Start Date). If current contact is inaccurate, please correct here:

Main Contact corrected name:

Main Contact corrected email:

Technical Administrator:

[redacted]

The Technical Administrator is the main contact for technical and system related communications. If current contact is inaccurate, please correct here:

Technical Administrator corrected name:

Technical Administrator corrected email:

Please provide a Financial Contact - The Financial Contact acts as the main Customer contact for finance related communication including invoicing.

Customer Financial Contact name:

Customer Financial Contact email:

5. CUSTOMER LOCATION

Customer has provided the following primary access location:

HMRC (Her Majesty's Revenue & Customs)

100 Parliament Street, SW1A 2BQ London, LO, United Kingdom

This is the primary (but not the only) location from which Customer will access the Cloud Service. Customer's failure to provide SAP with its VAT and/or GST number may have sales tax implications. If Customer does not provide a primary access location, SAP will incorporate a default primary access location to Customer's soldto address.

Customer's VAT/GST Number:

6. ADDITIONAL TERMS

The Agreement is subject to the following modifications:

6.1. Product Development Schedule

The Product Development Schedule published at http://sap.com/agreements-cloud-product-developmentschedule (which will be provided by SAP upon request upon or before execution of the Order Form) is incorporated into and becomes an integral part of the Order Form.

6.2. Governance

SAP and Customer agree that they will meet on a mutually agreed basis to review and discuss Customer's usage of the Cloud Services including the Usage Metrics and volume.

6.3. Replacement Order

The Initial Contracts dated December 22, 2016 and September 29, 2018 as subsequently amended by the Novation and Amendment Agreement previously entered into by the parties dated August 3, 2020 ("Prior Order") are hereby terminated effective as of the effective date of this Order Form, except for Consulting Services, if any currently being performed under the Prior Order. SAP shall provide Customer a credit for any prepaid unconsumed fees under the Prior Order. [redacted]

6.4. Summary on the Use of and Changes to Subprocessors

To provide the SAP Cloud Services under the Order Form, SAP relies on subprocessors. Some of them are SAP and SAP SE Affiliates and others are third party providers. In accordance with Data Protection laws, SAP provides Customer with the then-current list of Subprocessors used for the Cloud Services subscribed to under this Order Form at the following link https://support.sap.com/en/my-support/trust-center/subprocessors.html [See section 6.1 of the DPA]. For the avoidance of doubt, SAP may appoint and replace Subprocessors as per section 6.2 of the DPA. SAP will inform the Customer in advance (by email or by posting on the My Trust Center) of any intended additions or replacements to the list of Subprocessors [in accordance with Section 6.2 of the DPA]. Customer may receive notifications of these changes to Subprocessors by signing up to My Trust Center through the following link https://support.sap.com/content/dam/support/en_us/library/ssp/my-support/trust-center/sap-tc-04-0005.pdf. Customer may request that the parties discuss in good faith a resolution to the objection of the new Subprocessor (in accordance with Section 6.3(b) of the DPA). Without limitation, such discussions may include consideration of the impact (if any) on Customer's use of the Cloud Service and/or consideration of steps that could be taken to resolve Customer's objection. If Customer continues to object, Customer has the right to reject the appointment of a new Subprocessor within 30 days from the date SAP informs customer of the new Subprocessor [see Section 6.3(a) of the DPA] and, if the parties cannot resolve in good faith the objection, terminate the affected Cloud Service [see Section 6.3(a) of the DPA]. Such termination to be effective no later than twelve (12) months after the thirty (30) days notice period in section 6.3 of the DPA.

6.3 [redacted]

6.5. Location of Data Centers

As of the Order Form Effective Date, the production and test data centers used to host Customer Data for the Cloud Service are located within the Netherlands [redacted] and Germany [redacted]. SAP will not change the location of production or test data centers outside of the European Union without Customer's prior consent. If SAP

plans to migrate such a data center within the European Union SAP shall provide Customer written notice (email permitted) no later than 1 month before the planned migration.

Ariba Data Centers

Additionally, the data centers for the SAP Ariba Network are currently located in [redacted] California, USA [redacted] and in [redacted] Virginia, USA [redacted]. The SAP Ariba Network

facilitates and routes transactional data between SAP Ariba's buyer customers and their respective suppliers globally.

6.7. The Deployment Descriptions that apply to the Cloud Services under this Order Form are available in Ariba Connect through the following link https://connectsupport.ariba.com/sites#productknowledgedisplay&/?tab=Deployment_Descriptions

7. AMENDMENT TO THE GTC

The Agreement is subject to the following modifications:

With respect to this Order Form and solely with respect to the SAP Cloud Services (excluding third party Cloud Services) the parties agree the following amendments to the GTCs. For the avoidance of doubt any third-party Cloud Services provided under this Agreement shall be governed by the unamended General Terms and Conditions attached at Schedule G. In the event of any inconsistency, the terms set out in this Order Form shall prevail over the terms set out in the GTC. All other terms contained in the GTC shall remain in force.

7.1 A new definition shall be inserted at clause 1.15 as follows:

"Export Laws" means all applicable import, export control and sanctions laws, including without limitation, the laws of the United States, the EU, and Germany.

7.2 Clause 2.3. shall be amended with the insertion of the following at the end of the clause:

"Customer may use the Cloud Service world-wide, except Customer shall not use the Cloud Service from countries where such use is prohibited by Export Laws. Permitted uses and restrictions of the Cloud Service also apply to Cloud Materials and Documentation."

7.3 Clause 12.4. shall be deleted in its entirety and replaced with the following:

"Trade compliance

A) SAP and Customer shall comply with Export Laws in the performance of this Agreement. SAP Confidential Information is subject to Export Laws. Customer, its Affiliates, and Authorized Users shall not directly or indirectly export, re-export, release, or transfer Confidential Information in violation of Export Laws. Customer is solely responsible for compliance with Export Laws related to Customer Data, including obtaining any required export authorizations for customer data. Customer shall not use the cloud service from Crimea/Sevastopol, Cuba, Iran, The People's Republic of Korea (North Korea) or Syria.

B) upon SAP's request, Customer shall provide information and documents to support obtaining an export authorization. Upon written notice to Customer, SAP may immediately terminate Customer's subscription to the affected Cloud Service if (i) the competent authority does not grant such export authorization within eighteen months or (ii) Export Laws prohibit Sap from providing the Cloud Service to Customer."

8. DATA SUBJECT REQUESTS

8.1 The following sentence is deleted from Section 3.4 DPA (or similar):

"SAP shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable."

8.2 The preceding sentence is replaced by the following:

"To the extent permitted by Data Protection Law, if SAP receives a request from a Data Subject in relation to the Personal Data processing hereunder, SAP shall promptly notify Customer and shall not respond to such request itself but instead ask the Data Subject to redirect its request to Customer. In the event of a dispute with a Data Subject as it relates to SAP's processing of Personal Data under this DPA, the parties shall keep each other informed and, where appropriate, reasonably co-operate with the aim of resolving the dispute amicably with the Data Subject."

9. INTERNATIONAL TRANSFERS

9.1 Sections 7.2 to 7.4 of the DPA are deleted in their entirety and replaced by the following new Sections 7.2 to 7.5:

"7.2 Applicability of the Standard Contractual Clauses (2010)

7.2.1 Where for the period up to and including 26 September 2021, Personal Data of a Controller that is subject to GDPR is processed in a Third Country, or where Personal Data of a Swiss or United Kingdom based Controller or another Controller is processed in a Third Country and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses (2010):SAP and Customer enter into the Standard Contractual Clauses (2010); then:

Customer joins the Standard Contractual Clauses (2010) entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations; or

Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses (2010) with SAP or the relevant Subprocessors in the same manner as Customer in accordance with Sections 10,1 0 above. In such case, Customer will enter into the Standard Contractual Clauses (2010) on behalf of the other Controllers.

7.2.2 The Standard Contractual Clauses (2010) shall be governed by the law of the country in which the relevant Controller is established.

7.2.3 Where applicable Data Protection Law adopts the New Standard Contractual Clauses as meeting any required adequacy means as an alternative or update to the Standard Contractual Clauses (2010) then the New Standard Contractual Clauses shall apply in accordance with Section 7.3.

7.3 Applicability of New Standard Contractual Clauses

7.3.1 The following shall apply with effect from 27 September 2021 and shall solely apply in respect of New SCC Relevant Transfers:

7.3.1.1 Where SAP is not located in a Third Country and acts as a data exporter, SAP (or SAP SE on its behalf) has entered into the New Standard Contractual Clauses with each Subprocessor

as the data importer. Module 3 (Processor to Processor) of the New Standard Contractual Clauses shall apply to such New SCC Relevant Transfers.

7.3.1.2 Where SAP is located in a Third Country:

a) SAP and Customer hereby enter into the New Standard Contractual Clauses with Customer as the data exporter and SAP as the data importer which shall apply as follows:

i. Module 2 (Controller to Processor) shall apply where Customer is a Controller; and ii. Module 3 (Processor to Processor) shall apply where Customer is a Processor. Where Customer acts as Processor under Module 3 (Processor to Processor) of the New Standard Contractual Clauses, SAP acknowledges that Customer acts as Processor under the instructions of its Controller(s).

b. Other Controllers or Processors whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into the New Standard Contractual Clauses with SAP in the same manner as Customer in accordance with Section 07.3.1.2 above. In such case, Customer enters into the New Standard Contractual Clauses on behalf of the other Controllers or Processors.

7.3.2 With respect to a New SCC Relevant Transfer, on request from a Data Subject to the Customer, Customer may make a copy of Module 2 or 3 of the New Standard Contractual Clauses entered into between Customer and SAP (including the relevant Schedules), available to Data Subjects.

7.3.3 The governing law of the New Standard Contractual Clauses shall be the law of Germany.

7.4 Relation of the Standard Contractual Clauses to the Agreement

7.4.1 Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses (2010) or the New Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and Subprocessor rules, such specifications also apply in relation to the Standard Contractual Clauses (2010) and the New Standard Contractual Clauses.

7.5 Third Party Beneficiary Right under the New Standard Contractual Clauses

7.5.1 Where Customer is located in a Third Country and acting as a data importer under Module 2 or Module 3 of the New Standard Contractual Clauses and SAP is acting as Customer's sub-processor under the applicable Module, the respective data exporter shall have the following third party beneficiary right: In the event that the Customer has factually disappeared, ceased to exist in law or has become insolvent (in all cases without a successor entity that has assumed the legal obligations of the Customer by contract or by operation of law), the respective data exporter shall have the right to terminate the affected Cloud Service solely to the extent that the data exporter's Personal Data is processed. In such event, the respective data exporter also instructs SAP to erase or return the Personal Data.

10. ATTACHMENTS

10.1 For the purposes of the New Standard Contractual Clauses, Appendix 1 and Appendix 2 shall be referenced as Annex I and Annex II respectively.

10.2 The following Sections 1. to 3. are added to Appendix 1:

1. A. LIST OF PARTIES

In respect of the New Standard Contractual Clauses:

Module 2: Transfer Controller to Processor

Where SAP is located in a Third Country, Customer is the Controller and SAP is the Processor, then Customer is the data exporter and SAP is the data importer.

Module 3: Transfer Processor to Processor

Where SAP is located in a Third Country, Customer is a Processor and SAP is a Processor, then Customer is the data exporter and SAP is the data importer.

2. B. DESCRIPTION OF TRANSFER

2.1. In respect of the New Standard Contractual Clauses:

Module 2: Transfer Controller to Processor

Module 3: Transfer Processor to Processor

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Transfers shall be made on a continuous basis.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Personal Data shall be retained for the duration of the Agreement and subject to Section 4.2 of the DPA (Data retention).

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: Transfers to Subprocessors shall be on the same basis as set out in the DPA.

Special Data Categories (if agreed)

The transferred Personal Data may comprise special categories of personal data set out in the Agreement ("**Sensitive Data**"). SAP has taken Technical and Organizational Measures as set out in Schedule 2 to ensure a level of security appropriate to protect also Sensitive Data.

The transfer of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):

training of personnel;

encryption of data in transit and at rest;

system access logging and general data access logging.

In addition, the Cloud Services provide measures for handling of Sensitive Data as described in the Documentation.

3. C. COMPETENT SUPERVISORY AUTHORITY

3.1. Module 2: Transfer Controller to Processor

Module 3: Transfer Processor to Processor

In respect of the New Standard Contractual Clauses, where Customer is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the New Standard Contractual Clauses.

Accepted By:

HMRC (Her Majesty's Revenue & Customs)
(Customer)

Name:
Title:
Date:

SAP ARIBA AND FIELDGLASS CLOUD SERVICES SUPPLEMENTAL TERMS AND CONDITIONS

This Supplement is part of an Agreement for SAP products and services between SAP and Customer and applies to the SAP Ariba and Fieldglass Cloud Services for which Customer is subscribed as set forth herein (the "**Cloud Service**"). Capitalized terms used in this Supplement but not defined herein have the meanings assigned to them in the applicable Order Form or Documentation. Unless an alternate Supplemental Terms and Conditions document is referenced in the applicable Cloud Service Order Form, this Supplement applies to all SAP Ariba and Fieldglass Cloud Services as set forth herein whether or not referred to specifically in this Supplement.

PART 1 – SUPPLEMENTAL TERMS APPLICABLE TO ARIBA AND FIELDGLASS CLOUD SERVICES

1. CONSULTING SERVICES

Customer's initial subscription to each Cloud Service includes a standard Consulting Service package for the initial deployment of the Cloud Service, as applicable[1]. Such Consulting Service packages are not included with any additional, replacement, or renewal order of a Cloud Service to which Customer is already subscribed unless otherwise provided in the Order Form.

Standard Consulting Services for the initial deployment of applicable Cloud Services subscribed to in an Order Form between SAP and Customer referencing this Supplement are described in the deployment descriptions made available online by SAP, or as provided by SAP upon request. SAP provides these deployment services for the period stated in the deployment descriptions or applicable exhibit(s) or, if no period is stated, then for the initial Subscription Term. Any included deployment services, or other Consulting Services included in a Cloud Service Order Form between SAP and Customer referencing this Supplement, shall be deemed part of the Cloud Service for the purposes of the Cloud Service conformity and skill warranty in the GTC. The standard Consulting Service package included in Customer's initial subscription to each applicable Cloud Services expressly excludes any custom integration services or other custom development effort. Customer may purchase additional Consulting Services beyond the scope identified in the deployment description(s) for the initial deployment subscribed to Cloud Services by entering into a separate mutually agreeable written services order form or statement of work with SAP. Customer will reimburse SAP for all appropriately documented travel and related expenses incurred by SAP in performing any Consulting Services.

2. DATA

For clarity, this Section 2 shall be deemed an SAP Policy. Customer may not, and shall ensure its Authorized Users do not, submit the following types of information to the Cloud Service or solicit this information from trading partners: (i) non-public government identification numbers or financial account numbers associated with individual persons (e.g. U.S. Social Security numbers, national insurance numbers, driver's license numbers, or personal credit card or banking account numbers), (ii) medical records or health care claim information associated with individuals, including claims for payment or reimbursement for any type of medical care for an individual, (iii) information regulated under the International Traffic in Arms Regulations, (iv) without the express written consent of SAP, technical data restricted under U.S. or German law for export purposes, and (v) data designated as "Sensitive" or "Special Category" or the like requiring extra protective measures under the applicable Data Protection Law (as defined in the Data Processing Agreement). All Customer Data shall be considered Customer Confidential Information, provided, nothing in this Agreement shall restrict SAP from

[1] The following Cloud Service subscriptions do not include a standard Consulting Service package for the initial deployment of the Cloud Service: SAP Ariba Buying, additional site add on; SAP Ariba Buying and Invoicing, additional site add on; Buyer Membership (open adapter); Invoice Conversion Services; Services Invoicing for Brazil; Ariba Network, tax invoicing for Mexico; Ariba Network, tax invoicing for Chile; SAP Ariba Strategic Sourcing, supplemental site add-on; SAP Ariba Procurement, supplemental site add-on; SAP Signature Management by DocuSign; SAP Signature Management by DocuSign, Fieldglass; SAP Fieldglass Contingent Workforce Management (Trans); SAP Fieldglass Services Procurement (Trans)

freely using, reproducing, sharing, incorporating, exploiting and/or otherwise commercializing any feedback shared by Customer in any form for any purpose.

3. AGGREGATED USAGE

Where any Cloud Service is identified or marked in the Order Form as an 'aggregated' Usage Metric Limit over the Subscription Term (or 2 or more years thereof), SAP has agreed to an aggregated Usage Metric for the particular Cloud Service over the initial Subscription Term only. There is no discount, reduction, refund or credit if the Usage Metric Limit is not utilised in any year or over the Subscription Term. For any twelve (12) month renewal, the applicable Usage Metric Limit for the Cloud Service shall be annualised (subject always to excess use as provided in the Order Form) for the Renewal Term, unless otherwise agreed in a signed writing with SAP. The Annualised Usage Metric Limits may be set out in the Order Form as a reference.

4. LIMITED AVAILABILITY OF SELECT FEATURES

From time to time, subject to the requirements presented by SAP at the time, Customer may elect to participate in a limited availability program enabling use of a new feature for the Cloud Service prior to general production availability. SAP may elect at its own discretion to remove any limited availability feature from use and/or not release it into the Cloud Service.

PART 2 – SUPPLEMENTAL TERMS APPLICABLE TO FIELDGLASS CLOUD SERVICES ONLY

1. USAGE METRICS

Usage Metrics for the SAP Fieldglass Cloud Services, to the extent referenced in the Order Form, are defined as follows:

1.1. **"Spend"** means the total monetary amount processed by the Cloud Service.

1.2. "**Monitored Individuals**" means unique individuals being managed by the Cloud Service or who use the reporting console of the Cloud Service. This metric may also be referred to as "Worker Profile". For purposes of clarity, this Usage Metric is a monthly allotment, unless otherwise specified in the Order Form.

2. CLOUD SERVICE DESCRIPTION

Customer has subscribed to one or more of the Cloud Services described below in an Order Form referencing this Supplement.

2.1. **SAP Fieldglass Contingent Workforce Management.** SAP Fieldglass Contingent Workforce Management provides functionality for the procurement, engagement, and payment of contingent labor (e.g. job postings, approvals, candidate submissions, onboarding, off-boarding, invoices, and worker evaluations).

2.2. **SAP Fieldglass Assignment Management**. SAP Fieldglass Assignment Management provide functionality to track external resources for assignment to one or multiple projects, collect and process a resource's time, and allocate time to cost objects to support invoicing.

2.3. **SAP Fieldglass Services Procurement.** SAP Fieldglass Services Procurement provides functionality for the procurement, engagement, and payment of services providers (e.g. project requisitions, vendor responses, onboarding, off-boarding, invoicing, and project evaluation).

2.4. **SAP Fieldglass Worker Profile Management.** SAP Fieldglass Worker Profile Management allows Customers to track and manage all non-traditional workers who have no time sheet activity and are not otherwise tied to a job posting or SOW in the Cloud Service for headcount, reporting and onboarding/offboarding tasks.

2.5. **SAP Fieldglass SOW Worker and Documentation Tracking.** SAP Fieldglass SOW Worker and Documentation Tracking allows Customers to track and manage all nontraditional workers who have no time sheet activity and are not otherwise tied to a job posting or SOW in the Cloud Service for headcount, reporting and onboarding/offboarding and document tracking. It does not provide customers with the ability to track the financial management of services procurement such deliverables, fees, time sheets, expense sheets, or invoices.

3. SUPPORT

Support for the Cloud Service is provided in accordance with the Support Policy for SAP Cloud Services referenced in the Order Form. The support levels available for SAP Fieldglass are SAP Enterprise Support or Preferred Success. Preferred Care is not available. SAP Fieldglass Enterprise Support provides support for general questions, system navigation inquiries, general troubleshooting issues and P1 escalation management. In addition, SAP Fieldglass Enterprise Support provides release updates, high level program consultation, standard release notes and general product roadmap updates.

4. SUPPLIER TERMS

Prior to accessing the Cloud Service, Suppliers will be required to: (i) register through the Cloud Service; (ii) enter an agreement with SAP; and, if applicable, (iii) become enabled, subject to the applicable terms of use, on the regional network designated by SAP for routing documents between Customer and Suppliers. "Supplier" means a worker or agency engaged by Customer through the Cloud Service.

PART 3 – SUPPLEMENTAL TERMS APPLICABLE TO ARIBA CLOUD SERVICES ONLY

1. ARIBA SOLUTION DESCRIPTION GUIDE

The technology features included in each SAP Ariba Cloud Service are listed in the SAP Ariba Solution Description Guide (as updated from time to time).

2. SAP ARIBA PAYABLES

The SAP Ariba Payables (including the payment, supply chain finance, and discounting services) Cloud Service have regional limitations, may require agreements with third party service providers, and are subject additionally to the SAP Ariba Payables Supplemental Terms and Conditions found here: www.sap.com/agreements-cloud-supplement-ariba-payables (as updated from time to time).

3. ARIBA USAGE METRICS.

The Usage Metrics applicable to the Ariba Cloud Services are defined below.

3.1. **"Document(s)"** mean uniquely identified objects processed by the Cloud Service in a contract year.

3.2. **"Spend"** means the total monetary amount processed by the Cloud Service. For SAP Ariba Spend Analysis, "**Spend**" or "**Spend Data**" mean each twelve (12) month set of accounts payable, travel & expense, and/or purchasing card data from Customer provided to SAP for data enrichment processing through the Cloud Service, including transaction data and data identifying Customer's suppliers.

3.3. **"Supplier"** means a vendor from which Customer acquires goods or services for its own account using the Cloud Service.

3.4. "**User**" means individuals authorized to access the Cloud Service, excluding individuals who are only Team Members. The User Usage Metric is not measured as an aggregate number over a Subscription Period but rather as a limit that may not be exceeded at any time during the Subscription Period without being considered an excess usage.

3.5. "**Team Member**" means an individual who is allowed to access the Cloud Service but is only granted membership in groups associated with "Team Member" permissions for the Cloud Service.[2]

3.6. "**Tenant**" means a Customer-specific instance of the Cloud Service.

4. ADDITIONAL ARIBA TERMS.

4.1. **Quote Automation.** Customer's use of the Ariba Network and the Ariba Discovery Cloud Service as provisioned by the Quote Automation feature (if available via Customer's subscription) is limited to the use necessary to fully utilize the feature and as further described in the Documentation. In order to utilize the Quote Automation feature, Customer must register on the Ariba Discovery network and

[2] These permissions are found in the group licensing Reference table in the SAP Ariba *Strategic Sourcing and Supplier Management* portfolios descriptions found in the SAP Ariba Documentation.

accept the Terms of Use (Buyers) – Ariba Discovery in regards to functions of Quote Automation performed on the Ariba Discovery site.

4.2. **Ariba e-Archiving.** Ariba e-Archiving, an optional feature within the SAP Ariba Commerce Automation Cloud Service involves archiving of invoices originating from any one of the supported countries listed in the Documentation (each a "Supported Country") during the specified retention period for such Supported Country ("Mandatory Retention Period") and within Customer's Subscription Term.

4.3. **SAP Ariba Spot Buy Catalog Cloud Service and Feature.** In utilizing the SAP Ariba Spot Buy Catalog Cloud Service or using the SAP Ariba Spot Buy feature, Customer agrees to participate in the SAP Ariba Spot Buy Program in accordance with the terms for buyers found on the SAP Ariba Spot Buy program Site, as updated from time to time, (currently at https://connect.ariba.com/AribaSpotBuy).

4.4. **Supply Chain Collaboration for Buyers Cloud Service ("SCC for Buyers").** During the then-current Subscription Term for SCC for Buyers, SAP shall not charge any Customer suppliers transaction fees or annual membership fees related to Ariba Network Fulfill: Orders and Invoices service on the Ariba Network arising from their relationship or transactions between Customer and such suppliers originating through the SCC for Buyers. Suppliers will still be charged for use of Ariba Discovery if they elect to use that service or other optional services SAP makes available to them.

4.5. **SAP Ariba APIs, extension tools and Integration Software.** Some of the Cloud Services include the ability to use application programming interfaces, integration adapter software, extension capabilities and system authorization codes (together referred to as "**APIs**") made available by SAP for the creation of applications for integration with the Cloud Services by Customer (a "**Customer Application**").

i. Use of APIs is subject to restrictions stated in the Documentation and access to and testing of some APIs utilizes the regional SAP Ariba Developer Portal applicable to the SAP Ariba data center that Customer elects to use (See https://developer.ariba.com/api). Customer must accept any separate terms and conditions presented upon download or access to the regional platform to use the portal and APIs. ii. The APIs are SAP proprietary and Confidential Information and may not be modified by Customer.

iii. SAP may require certification, security assurances or other reasonable validation steps regarding the Customer Application(s) developed with the API prior to enabling Customer to utilize such application in a production capacity to exchange information with the Cloud Services.

iv. Customer is fully responsible for ensuring that the Customer Application remains compatible and interoperable with the Cloud Service and does not unreasonably impair, degrade or reduce the performance or security of the Cloud Service.

v. Customer will defend SAP against claims brought against SAP, SAP SE, its Affiliates and subcontractors by any third party arising from the Customer Application by virtue of its integration with the Cloud Service. 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. If Customer licensed the Cloud Services in the United Kingdom or is governed by the law of the United Kingdom, this Section v. of this Supplement is replaced in its entirety with the following v:

> "v Customer will defend SAP, any Affiliate of SAP, SAP SE, any Affiliate of SAP SE and any subcontractor of any of the foregoing against any claim brought by a third party in relation to the Customer Application. Customer will indemnify SAP, any Affiliate of SAP, SAP SE, any Affiliate of SAP SE and any subcontractor of any of the foregoing against all damages finally awarded (or the amount of any settlement entered into by any of the same) in relation to any claim brought by a third party related to the Customer Application. SAP shall be entitled to recover losses on behalf of any party afforded protection or indemnity under this section, however, Affiliates of SAP, SAP SE, Affiliates of SAP SE and subcontractors of any of the foregoing shall have the right to directly enforce the provisions of this section v for their own benefit under the Contracts (Rights of Third Parties) Act 1999 (provided there shall be no double recovery of losses permitted)."

vi. The System Availability SLA will apply to API's, unless specified otherwise in the Documentation for a specific API.

vii. For the avoidance of doubt, data submitted to the Cloud Services via an API or a data feed from an authorized third-party service that either originates with Customer or is provided subject to an agreement between Customer and a third-party database provider, shall be considered Customer Data under the Agreement.

4.6. **Data-as-a-Service Elements.** The following terms apply to SAP Ariba Spend Analysis Cloud Service, SAP Ariba Contract Management, SAP Ariba Sourcing and SAP Ariba Supplier Risk Cloud Service related to the information provided to Customer by SAP, which may include news articles, supplier corporate information, ("**Database Information**"). All Database Information provided to Customer is proprietary information of SAP or

its third-party information providers, may not be relicensed or resold and is subject to further restrictions set forth in the Documentation. The Database Information is provided "as is" without warranty of any kind, including but not limited to warranties as to the accuracy, completeness or timeliness of the Database Information, and SAP advises Customer to independently verify such Database Information. SAP and its providers shall not be liable for any loss arising out of or in any way relating to the Database Information. SAP's Providers are third party beneficiaries of these terms. SAP and its Providers (i) shall not be liable to Customer for any loss or injury arising out of or in any way relating to the Database Information and (ii) will not be liable for consequential, incidental, special, punitive or other indirect damages.

4.7. **Optional Add-on Services**. Customer may subscribe to certain optional add-on services or programs, such as "Ariba Network, add-on for buyer-paid supplier fees for orders and invoices" and Ariba Discovery Advantage Block Purchase. If so, any Usage Metrics or terms not stated in this Supplement will be stated in the Order Form or Documentation.

4.8. **Data Retention – Ariba Network**. Customer Data processed on the Ariba Network may be retained on the Ariba Network subject to SAP's policies, provided that SAP Ariba will delete, or render unreadable, the Customer Data stored in the Ariba Network after expiration or termination of Customer's subscription upon Customer's written request. Retained data is subject to the confidentiality provisions of the Agreement and the obligations under the Data Processing Agreement.

4.9. **Processing Services for Payment and Supply Chain Finance**.

4.9.1. **Separate Provider**. If Customer enables one or more of the below defined payment capabilities in the Ariba Network (excluding AribaPay), such payment services are provided by third party payment processors under separate agreements between Customer and those third-parties. SAP does not perform and is not responsible for the payment processing services, nor acts or omissions of the third-party payment processors under the separate agreements. Customer agrees that any third-party payment processor's use of Customer Data is governed by the separate agreement and the third-party payment processor's data use and data privacy policies. By enabling the payment services provided by third-party payment processors, Customer instructs SAP to transfer Customer Data (including personal data) to the third-party payment processor. SAP's obligations for the Cloud Service, exclusive of the payment processing services, are in accordance with the Agreement. SAP and the third-party payment processors are under no obligation to assist with or resolve disputes between Customer and Customer's suppliers, with respect to payment transactions.

4.9.2. **Payment Processing Services**. For payment processing services other than AribaPay:

- If Customer enables the payment capability, then the "processing services" consist of payment processing services to settle payments between Customer and Customer's suppliers, including every function of the payment capability related to the processing or transmission of payments or funds, the provision of any payment intermediary-related services, the debiting or crediting of bank accounts, holding funds, processing payments, issuing checks, holding account numbers, and/or otherwise acting as a payment processor.
- Customer is responsible for providing accurate information in any payment instruction.
- Once enabled, SAP's role for the payment capability is to forward payment information from Customer to the payment processor and return status information to the Customer regarding the payments.

4.9.3. **Tax Treatment.** With respect to the fees payable by Customer to SAP for use of the payment capability, Customer will be treated as the payor with respect to SAP for tax purposes, notwithstanding the payment processing services provided by the payment processor or supply chain finance processor. This will not include features which are agreed to by Customer under its agreement with the payment processor payment and that are paid directly to the payment processor.

4.10. **Packaged Cloud Service**. Where the Cloud Service is included with SAP Qualtrics for Supplier XM for a single fee (collectively, the "**Packaged SAP Qualtrics Cloud Service**"), the following additional terms apply to such Packaged SAP Qualtrics Cloud Service:

4.10.1. **Usage Metric and Limitations for SAP Ariba Strategic Sourcing Suite**. Subscriptions to the Packaged SAP Qualtrics Cloud Service which includes SAP Ariba Strategic Sourcing Suite are measured by Users and include 50 Suppliers per User in blocks of 25 Suppliers.

4.10.2. **Usage Metric and Limitations for SAP Ariba Commerce Automation Membership**. Subscriptions to the Packaged SAP Qualtrics Cloud Service which includes SAP Ariba Commerce Automation Membership include 1,000 Suppliers in blocks of 25 Suppliers (for a total of 40 blocks of 25 Suppliers).

4.10.3. **Usage Metric and Limitations for SAP Ariba Supply Chain Collaboration for Buyers**. Subscriptions to the Packaged SAP Qualtrics Cloud Service which includes SAP Ariba Supply Chain Collaboration for Buyers are measured in blocks of $10M in Spend and include 25 Suppliers for each block of $10M in Spend.

4.10.4. **EU Access**. The EU Access option is not available for the Packaged SAP Qualtrics Cloud Service.

4.10.5. **Customer Data Deletion**. Customer is responsible for deleting all Customer Data for SAP Qualtrics for Supplier XM upon termination. SAP will provide Customer a means to accomplish such deletion.

4.10.6. **Support**. The Contact Channel for support for SAP Qualtrics for Supplier XM is https://www.qualtrics.com/support/. If SAP changes the Contact Channel, SAP will provide notice via https://www.qualtrics.com/support/. All other aspects of support are provided in accordance with SAP's Support Policy for Cloud Services.

SAP Signature Management by DocuSign Supplemental Terms and Conditions

This Supplement is part of an Agreement for SAP Cloud Services between SAP and Customer and applies only to SAP Signature Management by DocuSign (the "Cloud Service"). Any documents referenced in this Supplement are available upon request.

1. CLOUD SERVICE

1.1. **Service.** The Cloud Service supports customers to upload documents to the Cloud Service and to collect and manage signatures on such documents through workflows established by the customer. There are three editions of the Cloud Service: SAP Signature Management by DocuSign, basic edition; SAP Signature Management by DocuSign, premium edition; and SAP Signature Management, government compliance option.

1.2. **Add-Ons.** Two add-on services are available with SAP Signature Management by DocuSign, premium edition and SAP Signature Management, government compliance option: SAP Signature Management by DocuSign, add-on for Part 11 regulations and SAP Signature Management by DocuSign, add-on for standards-based signature compliance. One add-on service is available with SAP Signature Management by DocuSign, basic edition: SAP Signature Management by DocuSign, add-on for standards-based signature compliance.

2. USAGE METRIC

2.1. The Usage Metric for the Cloud Service is Transactions per Contract Year, in blocks of 100. Transactions are all jobs submitted to the Cloud Service in a Contract Year. Transactions also include those jobs sent via bulk or using Powerform, both of which are only available in SAP Signature Management by DocuSign, premium edition and SAP Signature Management, government compliance option. "Powerform" means a Transaction that may be accessed and completed by accessing a hyperlink (i.e. which does not need to be individually sent to each recipient). A Contract Year means a 12-month period beginning on the first day of the Subscription Term or its annual anniversary.

3. ADDITIONAL TERMS

3.1. **Content.** No Customer Data is entered into the Cloud Service except to the extent included on a document uploaded to the Cloud Service or as required to include signatories of a document in Customer-established workflows. Documents are encrypted in the Cloud Service and neither SAP nor its third-party vendors have access to the content of such documents.

3.2. **Access**. The use of the Cloud Service in conjunction with SAP or third-party cloud services or software is limited to use cases associated with the SAP cloud service identified in the SAP Signature Management by DocuSign product name. However, use of the Cloud Service in connection with Salesforce.com is not permitted and requires additional license rights which need to be obtained directly by Customer from DocuSign Inc.

3.3. **Test Tenant.** Cloud Service includes one test tenant. The test tenant may only be used for non-productive testing of Cloud Service, and Customer may not process any personal data using the test tenant. The Service Availability SLA does not apply to the test tenant.

3.4. **Overuse**. SAP shall have the right to suspend Customer's access to the Cloud Service if Customer is over-consuming the amount of Usage Metric stated in the Order Form by more than 20%, until Customer subscribes to Usage Metrics in an additional Order Form sufficient to cover such excess use.

3.5. **Optional Quick Start Engagement from DocuSign.** Customer is entitled to receive up to 2-hours of consultation with a DocuSign engagement representative to explain account set up, permissions and administrator details (excludes add-ons). This engagement does not include implementation services. Customer must utilize this engagement within 180 days after the Agreement effective date.

SUPPORT POLICY FOR SAP CLOUD SERVICES

This Support Policy for SAP Cloud Services is part of an Agreement for certain SAP Cloud Services ("Agreement") between SAP and Customer.

SUPPORT AND SUCCESS PLAN SERVICES

As part of SAP's ONE Support approach, which provides a consistent support experience for Cloud Services and on-premise solutions, SAP offers the following support levels; SAP Enterprise Support, cloud editions, SAP Preferred Success and SAP Preferred Care. SAP Enterprise Support, cloud editions is included in the subscription fees for SAP Cloud Services stated in the Order Form unless alternative support terms are specified in the Supplemental Terms for the Cloud Service. SAP Preferred Success and SAP Preferred Care is offered for an additional fee, as an add-on to SAP Enterprise Support, cloud editions, for certain SAP Cloud Solutions listed under https://support.sap.com/preferredsuccessproductlist. SAP Preferred Success and SAP Preferred Care are not available, and are not provided, for any third-party cloud services purchased through SAP.

1. SCOPE OF THE SUPPORT AND SUCCESS PLAN SERVICES

Capitalized Terms are further defined in the table below. The support services are available in English language, unless stated otherwise.

1.1 Enterprise Support, cloud editions: Foundational engagement support with focus on customer interaction and issue resolution.

SAP Enterprise Support, cloud editions	
Mission Critical Support	
24x7 Mission Critical Support for P1 and P2 issues (English only)	✓
Non-Mission Critical Support for P3 and P4 issues during business hours (English only)	Monday to Friday 8 am to 6 pm (Local Time Zone), excluding local holidays
Customer Interaction Center 24x7	✓ (as stated below)
Global Support Backbone	✓
End-to-end Supportability	✓
Learning and Empowerment	
Access to remote SAP support content and services, e.g., Meet-the-Expert Sessions	✓
Release Update Information	Self-service through web and community
Collaboration	
SAP Support Advisory Services	✓
Support via web and platform for social business collaboration	✓
Support via chat during business hours in English language for non-Mission Critical Support issues	Currently available for SAP SuccessFactors, SAP Concur, SAP Ariba, SAP Business by Design, SAP Cloud for Customer and SAP S/4HANA Cloud Services

SAP Enterprise Support Reporting	✓
Innovation and Value Realization	
Proactive Checks proposed by SAP	✓
Product Roadmap Update Information	Self-service through web
Refresh of test instance	Self-service or request through web for initiating the refresh as offered and required by respective solution

1.2 SAP Preferred Success: An add-on to SAP Enterprise Support, cloud editions that includes strategic guidance, solution-specific best practices and Success Programs to help drive consumption 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 during business hours (English only)	Monday to Friday 8 am to 6 pm (Local Time Zone), excluding local holidays
Customer Interaction Center 24x7	✓ (as stated below)
Global Support Backbone	✓
End-to-end Supportability	✓
Learning and Empowerment	
Access to remote SAP support content and services, e.g., Meet-the-Expert Sessions	Access to SAP Preferred Success specific learning content. Customer can have up to 5 Key Users access SAP Learning Hub, solution edition specific to the cloud service
Release Update Information	Solution-specific Release Update Information
Collaboration	
SAP Support Advisory Services	✓
SAP Cloud Service and process-related guidance	Access to Success Resources for full customer lifecycle from onboarding to consumption, including technical and product usage advice, best practices and operational excellence, may include in-person delivery, at SAP's discretion
Regular checkpoint	Access to Success Resources to answer questions related to critical issues, reporting and best practices, may include in-person delivery, at SAP's discretion
Support via web and platform for social business collaboration	Exclusive access to SAP Preferred Success Community
Support via chat during business hours in English language for non-Mission Critical Support issues	Currently available for SAP SuccessFactors, SAP Cloud for Customer and SAP S/4HANA Cloud Services
SAP Enterprise Support Reporting	Enhanced Success Reporting
Innovation and Value Realization	
Access to Success Programs	✓
Proactive Checks proposed by SAP	Automated or self-service Proactive Checks for the specific solution in use

Product Roadmap Update Information	Solution-specific Product Roadmap Update Information
Periodic Cloud Service Review and Planning	Access to Success Resources for checkpoints, cycle planning, challenges and consumption planning, may include in-person delivery, at SAP's discretion
Refresh of test instance	Access to SAP assistance with managing the refreshing of test instances up to two times per year, where applicable

1.3 SAP Preferred Care: An add-on to SAP Enterprise Support, cloud editions that includes strategic guidance and customer-specific best practices to help 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 during business hours (English only)	Monday to Friday 8 am to 6 pm (Local Time Zone), excluding local holidays
Customer Interaction Center 24x7	✓ (as stated below)
Global Support Backbone	✓
End-to-end Supportability	✓
Learning and Empowerment	
Access to remote SAP support content and services, e.g., Meet-the-Expert Sessions	✓
Release Update Information	Customer-specific Release Update Information
Collaboration	
SAP Support Advisory Services	✓
SAP Cloud Service and process-related guidance	Access to Support Expert for technical and product usage advice, best practices and operational excellence (within customer's region)
Regular Checkpoint	Meeting with Support Expert to review critical issues, reporting 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	Currently available for SAP SuccessFactors, SAP Concur, SAP Ariba, SAP Business by Design and SAP S/4HANA Cloud Services
SAP Enterprise Support Reporting	✓
Innovation and Value Realization	
Proactive Checks proposed by SAP	Customer-specific Proactive Checks
Product Roadmap Update Information	Customer-specific Product Roadmap Update Information
Periodic Cloud Service Review And Planning	Meeting with Support Expert to discuss checkpoint, cycle planning, challenges and adoption plan

Refresh of test instance	Access to SAP assistance with managing the refreshing of test instances up to two times per year, where applicable.

1.4 Access to Empowerment and Innovation and Value Realization Services.

Empowerment content and session schedules are stated at the SAP Support Portal in the SAP Enterprise Support Academy section. Scheduling, availability and delivery methodology is at SAP's discretion.

Support services related to Empowerment and Innovation and Value Realization as stated above require a customer request and are 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 they may be deployed for a customer´s business process requirements, or giving a customer guidance in the form of knowledge transfer sessions. Scheduling, availability and delivery methodology are at SAP´s discretion.

2. CUSTOMER INTERACTION CENTER LANGUAGES

SAP Support provides initial telephone contact for Customer Contacts through the SAP one support phone number "CALL-1-SAP" (as stated at the CALL-1-SAP page: https://support.sap.com/contactus) and/or via other solution specific hotlines in the following languages: English (available 24 hours all weekdays) and, depending on local office hours and availability, in German, French, Italian, Spanish, Polish, Russian (during European office hours); Japanese, Chinese, Korean, Bahasa (during Asia/Pacific office hours); Portuguese and Spanish (during Latin America office hours). Issues which lead to a support case which is processed by specialized technical support engineers around the world or any support by a third party are in English only.

3. CONTACTING SUPPORT

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

For contacting SAP's support organization, the current preferred contact channel for SAP Enterprise Support, cloud editions is the SAP Support Portal at https://support.sap.com, unless otherwise set forth in the table below.

SAP Cloud Service	Contact Channels
SAP Concur	https://concursolutions.com
SAP Ariba	https://connect.ariba.com
SAP Fieldglass	https://www.fieldglass.com/customer-support or embedded in the application help menu
SAP Digital Interconnect	https://community.sapmobileservices.com/support (integrated scenarios use SAP Support Portal)
SAP Business ByDesign SAP Cloud for Customer SAP Learning Hub	Embedded in the applicable SAP Cloud Service: • For end-users: The "Help Center", accessible from every screen, • For Key Users: The "Application & User Management Work Center".

Customers that have an assigned Support Expert may contact them directly for solution expertise support.

4. 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	**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. This is generally caused by the following circumstances: - 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. A workaround is not available for each circumstance. The incident requires immediate processing because the malfunction may cause serious losses.	**Initial Response:** Within one hour of case submission. **Ongoing Communication:** Unless otherwise communicated by SAP Support, once every hour. **Resolution Target:** SAP to provide for issues either a (i) resolution, or (ii) workaround or (iii) action plan within four hours.
P2	**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. The incident is to be processed as quickly as possible because a continuing malfunction can seriously disrupt the entire productive business flow.	**Initial Response:** Within four hours of case submission for SAP Enterprise Support, cloud edition customers and within two hours of case submission for SAP Preferred Success and SAP Preferred Care customers. **Ongoing Communication:** Unless otherwise communicated by SAP Support, once every six hours. **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 Success and SAP Preferred Care customers only.
P3	**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.	**Initial Response:** Within one business day of case submission for SAP Enterprise Support, cloud edition customers, and within four business hours of case being received for SAP Preferred Success and SAP Preferred Care customers. **Ongoing Communication:** Unless otherwise communicated by SAP Support, once every three business days for Non-Defect Issues and ten business days for product defect issues.
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 submission for SAP Enterprise Support, cloud editions customers and within one business day of case submission for SAP Preferred Success and SAP Preferred Care customers. **Ongoing Communication:** Unless otherwise communicated by SAP Support, once every week.

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 those developed by SAP Custom Development and/or by SAP subsidiaries, or

individual content services); (ii) the root cause behind the incident is not a malfunction, but missing functionality ("development request") or the incident is ascribed to a consulting request ("how-to").

5. CUSTOMER'S RESPONSIBILITIES

5.1 Customer Contact. In order to receive support hereunder, Customer will designate at least two and up to five qualified English speaking contact persons (each a "Customer Contact", "Designated Support Contact", "Authorized Support Contact", "Key User" or "Application Administrator" – system administrator roles within specific Cloud Services) who are authorized to contact or access the Customer Interaction Center, SAP Support Advisory Services and Mission Critical Support services. The Customer Contact is responsible for managing all business-related tasks of the Cloud Service related to Customer's business, such as:

(i) Support end users and manage their incidents. This includes searching for known solutions in available documentation and liaising with SAP support in the event of new problems;

(ii) Manage background jobs and the distribution of business tasks across users (if available);

(iii) Manage and monitor connections to Customer's third-party systems (if available); (iv) Support the adoption of the Cloud Service.

5.2 Contact Details. Customer will provide contact details (in particular, e-mail address and telephone number) through which the Customer Contact or the authorized representative of the Customer Contact can be contacted at any time. Customer will update its Customer Contacts for an SAP Cloud Service through the SAP Support Portal at https://support.sap.com or the respective contact channel mentioned in section "Contacting Support" above. Only authorized Customer Contacts may contact SAP's support organization.

5.3 Cooperation. To receive support services, Customer will reasonably cooperate with SAP to resolve support incidents, and will have adequate technical expertise and knowledge of its configuration of the SAP Cloud Services to provide relevant information to enable SAP to reproduce, troubleshoot and resolve the experienced error such as e.g. reference ID, issue examples, screenshots.

6. CAPITALIZED TERMS

Below are further explanations of the capitalized terms used above:

Customer Interaction Center 24x7	Units within SAP's support organization that customers may contact for general support related inquiries through the described contact channels.
End-to-end Supportability	Support for incidents that occur in integrated business scenarios consisting of SAP Cloud Services and / or both SAP Cloud Services and other SAP products with a valid support agreement.
Enhanced Success Reporting	Enhanced Success Reporting means access to reports, dashboards, or other reporting components and capabilities regarding the overall engagement, full customer lifecycle, and productive use of the solution, including product consumption, technical and product usage, status of support services, and the achievements hereunder.
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 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).
Non-Defect Issue	A reported support case that does not involve a defect in the applicable SAP Cloud Service and does not require engineering / development or operations personnel to resolve.
Periodic Cloud Service Review and Planning	Periodic review of key business milestones and objectives for solutions covered under SAP Preferred Care and/or SAP Preferred Success.
SAP Preferred Success Communities	Social media-based empowerment and collaboration, aligning access to peers and SAP experts.
Proactive Checks	Support-services, providing recommendations for the specific customer situation.
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.
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 Reporting	A report or dashboard analyzing and documenting the status of support services and achievements hereunder (e.g., based on solution monitoring capabilities and support case status).

SAP Support Advisory Services	Access to experts who help customers on support-related requests and advice on the right support deliverables and assets.
Support Expert	A specific SAP customer representative (often referred to as Customer Success Manager) that is assigned to Customers as the primary contact for ongoing management, to provide support case oversight, technical guidance and mentorship, customer-specific information on release updates and guidance on adoption and usage.
Success Resources	Access to automated, guided or direct analysis, reporting, expertise, and knowledge components to drive operational excellence throughout the full customer lifecycle including onboarding, consumption, utilization and operations, as well as technical and product usage. At SAP's discretion, this may include a Support Expert.
Success Programs	A combination or integration of various Success Resources, learning content and platforms (e.g. webinars, chat sessions, etc.), and social business collaboration channels (e.g. communities) delivered in a programmatic or prescriptive approach that support successful deployment, consumption and ongoing value realization.

Schedule C

SERVICE LEVEL AGREEMENT FOR SAP CLOUD SERVICES

1. DEFINITIONS

1.1. **"Credit"** means 2% of Monthly Subscription Fees for each 1% below the System Availability SLA**,** not to exceed 100% of Monthly Subscription Fees**.**

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

1.3. "**Excluded Downtime**" means the Total Minutes in the Month attributable to a Maintenance Window; or any Major Upgrade Window for which the Customer has been notified at least five (5) business days in advance; or 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.

1.4. "**Maintenance Window**" means the weekly maintenance windows for the Cloud Service identified in https://support.sap.com/maintenance-windows. SAP may update the Maintenance Window from time to time in accordance with the Agreement.

1.5. **"Major Upgrade Window"** means the extended upgrade maintenance windows for the Cloud Service identified in https://support.sap.com/maintenance-windows. SAP may update the Major Upgrade Window from time to time in accordance with the Agreement.

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

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

1.8. "**System Availability Percentage**" is calculated and defined as follows:

$$\frac{\text{Total Minutes in the Month} - \text{Excluded Downtime} - \text{Downtime}}{\text{Total Minutes in the Month} - \text{Excluded Downtime}} * 100$$

1.9. "**System Availability SLA"** means a 99.7% System Availability Percentage during each Month for the production version of the Cloud Service.

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

1.11. "**UTC**" means Coordinated Universal Time standard being the start time for the applicable Maintenance Window and Major Upgrade Window.

2. SYSTEM AVAILABILITY SLA AND CREDITS

2.1. Credit

If SAP fails to meet the System Availability SLA for a particular Month, Customer may claim a Credit, which Customer may apply to a future invoice relating to the Cloud Service that did not meet the System Availability SLA (subject to Sections 2.1.1 and 2.1.2 below).

2.1.1. Claims for a Credit must be made in good faith and through a documented submission of 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 for the Cloud Service.

2.1.2. Customers who have not subscribed to the Cloud Service directly from SAP must claim the Credit from their applicable SAP partner.

2.2. System Availability Report

SAP will provide Customer with a monthly report describing the System Availability Percentage for the Cloud Service either by email following a request to Customer's assigned SAP account manager; through the Cloud Service; or through an online portal made available to Customer, if and when such online portal becomes available.

3. CHANGES TO WINDOWS

If Customer wishes to be notified of changes to Maintenance Windows and Major Upgrade Windows, it must subscribe to receive notifications at https://support.sap.com/maintenance-windows.

PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

1. BACKGROUND

1.1 Purpose and Application. This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer. This DPA applies to Personal Data processed by SAP and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SAP, and Customer shall not store Personal Data in such environments.

1.2 Structure. Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures.

1.3 GDPR. SAP and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

1.4 Governance. SAP acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use SAP as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

2. SECURITY OF PROCESSING

2.1 Appropriate Technical and Organizational Measures. SAP has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

2.2 Changes. SAP applies the technical and organizational measures set forth in Appendix 2 to SAP's entire customer base hosted out of the same Data Center and receiving the same Cloud Service. SAP may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3. SAP OBLIGATIONS

3.1 Instructions from Customer. SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented

initial instructions and each use of the Cloud Service then constitutes further instructions. SAP will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or SAP otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted).

3.2 Processing on Legal Requirement. SAP may also process Personal Data where required to do so by applicable law. In such a case, SAP shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

3.3 Personnel. To process Personal Data, SAP and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. SAP and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

3.4 Cooperation. At Customer's request, SAP will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data or any Personal Data Breach. SAP shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. SAP shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, SAP will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

3.5 Personal Data Breach Notification. SAP will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SAP may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SAP.

3.6 Data Protection Impact Assessment. If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SAP will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

4. DATA EXPORT AND DELETION

4.1 Export and Retrieval by Customer. During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal 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 Personal Data.

4.2 Deletion. Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs SAP to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless applicable law requires retention.

5. CERTIFICATIONS AND AUDITS

5.1 Customer Audit. Customer or its independent third party auditor reasonably acceptable to SAP (which shall not include any third party auditors who are either a competitor of SAP or not suitably qualified or independent) may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:

(a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other

SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or SAP;

(b) A Personal Data Breach has occurred;

(c) An audit is formally requested by Customer's data protection authority; or

(d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.

5.2 Other Controller Audit. Any other Controller may audit SAP's control environment and security practices relevant to Personal Data processed by SAP in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SAP on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

5.3 Scope of Audit. Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to SAP.

5.4 Cost of Audits. Customer shall bear the costs of any audit unless such audit reveals a material breach by SAP of this DPA, then SAP shall bear its own expenses of an audit. If an audit determines that SAP has breached its obligations under the DPA, SAP will promptly remedy the breach at its own cost.

6. SUBPROCESSORS

6.1 Permitted Use. SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

(a) SAP or SAP SE on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. SAP shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

(b) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

(c) SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the Cloud Service.

6.2 New Subprocessors. SAP's use of Subprocessors is at its discretion, provided that:

(a) SAP will inform Customer in advance (by email or by posting on the support portal available through SAP Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and **(b)** Customer may object to such changes as set out in Section 6.3.

6.3 Objections to New Subprocessors.

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SAP's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.

(b) Within the thirty day period from the date of SAP's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good

faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect SAP's right to use the new Subprocessor(s) after the thirty day period.

(c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

6.4 Emergency Replacement. SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 6.3 applies accordingly.

7. INTERNATIONAL PROCESSING

7.1 Conditions for International Processing. SAP shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

7.2 Standard Contractual Clauses. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

(a) SAP and Customer enter into the Standard Contractual Clauses;

(b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by SAP) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when SAP has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c), or a notice to Customer; and/or

(c) Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses with SAP and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.

7.3 Relation of the Standard Contractual Clauses to the Agreement. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.4 Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

8. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

9. EU ACCESS

9.1 Optional Service. EU Access is an optional service that may be offered by SAP. SAP shall provide the Cloud Service eligible for EU Access solely for production instances in accordance with this Section 9. Where EU Access is not expressly specified and agreed in the Order Form, this Section 9 shall not apply.

9.2 EU Access. SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service and SAP shall not export Personal Data outside of the EEA or Switzerland unless expressly authorized by Customer in writing (e-mail permitted) on a case by case basis; or as excluded under Section 9.4.

9.3 Data Center Location. Upon the effective date of the Agreement, the Data Centers used to host Personal Data in the Cloud Service are located in the EEA or Switzerland. SAP will not migrate the Customer instance to a Data Center outside 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 will notify Customer in writing (email permitted) no later than thirty days before the planned migration.

9.4 Exclusions. The following Personal Data is not subject to 9.2 and 9.3:

(a) Contact details of the sender of a support ticket; and

(b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymize that Personal Data before any transmission of the incident message to SAP.

10. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

10.1 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

10.2 "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/ourcompany/policies/data-privacy-and-security/location-of-data-center.html or notified to Customer or otherwise agreed in an Order Form.

10.3 "Data Protection Law" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by SAP on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

10.4 "Data Subject" means an identified or identifiable natural person as defined by Data Protection Law.

10.5 "EEA" means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

10.6 "European Subprocessor" means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

10.7 "Personal Data" means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by SAP or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

10.8 "Personal Data Breach" means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

10.9 "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.

10.10 "Standard Contractual Clauses" or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply).

10.11 "Subprocessor" means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP , SAP SE or SAP SE's Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Data Exporter
The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.

Data Importer
SAP and its Subprocessors provide the Cloud Service that includes the following support:

SAP SE Affiliates support the Cloud Service data centers remotely from SAP facilities in St. Leon/Rot (Germany), India and other locations where SAP employs personnel in the Operations/Cloud Delivery function. Support includes:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

SAP SE Affiliates provide 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. SAP answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data Subjects
Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service.

Data Categories
The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, email address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service and may include bank account data, credit or debit card data.

Special Data Categories (if appropriate)
The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any.

Processing Operations / Purposes
The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- provision of Consulting Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any fixes or upgrades 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
- execution of instructions of Customer in accordance with the Agreement.

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 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 employees and external personnel must wear their ID cards at all SAP locations. Additional measures for Data Centers:
- 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 protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.

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

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy
- All personnel access SAP's systems with a unique identifier (user ID).
- SAP has procedures in place so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization).

  In case personnel leaves the company, their access rights are revoked.
- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and 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 the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

- The company network is protected from the public network by firewalls.
- SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control. Persons entitled to use data processing systems 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:

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.
- SAP does not allow the installation of software that has not been approved by SAP.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at SAP to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center).

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems.

Measures:

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.

1.6 Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

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

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss. Measures:

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
- Emergency processes and systems are regularly tested.

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

Measures:

- SAP uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities. Measures:

- SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
- In particular, SAP uses the following to implement the control and measure sections described above:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.

Article of GDPR	Section of DPA	Click on link to see Section
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(2), 28(3) (d) and 28 (4)	6	SUBPROCESSORS
28 (3) sentence 1	1.1 and Appendix 1, 1.2	Purpose and Application. Structure.
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel.
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(3) (e)	3.4	Cooperation.
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organizational Measures. Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (g)	4	Data export and Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) (c)	7.2	Standard Contractual Clauses.

HM Revenue & Customs

Schedule 1

AUTHORITY'S MANDATORY TERMS

A. For the avoidance of doubt, references to 'the Agreement' means the Order Form for SAP Cloud Services SAP Reference No. 3061788005 ("**Order Form**") between the Supplier and the Authority.

References to 'the Authority' mean 'the Buyer' (the Commissioners for Her Majesty's Revenue and Customs).

B. The Agreement incorporates the Authority's mandatory terms set out in this Schedule 1 and any terms not defined herein will have the meanings given in the Agreement.

C. In case of any ambiguity or conflict, the Authority's mandatory terms in this Schedule 1 will supersede any other terms in the Agreement.

1. Definitions

"Affiliate" means, in relation to:

(a) the Supplier, any legal entity in which a party, directly or indirectly, holds more than a fifty percent (50%) of the shares or voting rights or control or is under common Control with that legal entity; and

(b) the Authority, the ALB (arm's length bodies), NDPB (non-department public bodies) and other associated departments or organisations that sit under the Control of HMRC. Any such entity shall be considered an HMRC Affiliate for only such time as HMRC continues to control such entity.

"Authority Data" means:

(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:

(i) entered into the Service by Authority or its Affiliates; and/or

(ii) End User specific data which is derived from the Authority's use of the Service as long as such derivative work is not a component of the Service itself or is not furnished by SAP under the Agreement; or

(b) any Personal Data for which the Authority is the Controller.

"Charges" means the charges for the Services as specified in Order Form (ref: 3061807645).

"Connected Company" means, in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person;

"Control" means, with regards to Supplier means the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly; and with regards to the Authority means having the ability to control budgets of the affiliate, having statutory responsibility for the affiliate or to control the management, procurement process and policies of such entity. Any such entity shall be considered an Affiliate for only such time as Authority continues to control such entity.

"Controller", "Processor", "Data Subject",	take the meaning given in the DPA.
"Data Protection Agreement" or **"DPA"**	has the meaning given in the Order Form.
"Data Protection Law"	means: (a) "the data protection legislation" as defined in section 3(9) of the Data Protection Act 2018; and; (b) all applicable Law protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.
"Key Subcontractor"	means any Subcontractor: (a) which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or (b) with a Subcontract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten per cent (10%) of the aggregate Charges forecast to be payable under this Call-Off Contract.
"Law"	means any applicable Act of Parliament, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply.
"Personal Data"	has the meaning given in the DPA.
"Purchase Order Number"	the Authority's unique number relating to the supply of the Services.
"Services"	means the hosted, on-demand solution provided by SAP under the Order Form, including upgrades and updates thereto made generally available by SAP to its customers.
"Subcontract"	means any contract or agreement (or proposed contract or agreement) between the Supplier (or a Subcontractor) and any third party whereby that third party agrees to provide to the Supplier (or the Subcontractor) all or any part of the Services, or facilities or services which are material for the provision of the Services, or any part thereof or necessary for the management, direction or control of the Services or any part thereof.

"Subcontractor"	means any third party with whom: (a) the Supplier enters into a Subcontract; or (b) a third party under (a) above enters into a Subcontract, or the servants or agents of that third party.
"Supplier Personnel"	means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier's obligations under the Agreement.
"Supporting Documentation"	sufficient information in writing to enable the Authority to reasonably verify the accuracy of any invoice.
"Tax"	means: (a) all forms of tax whether direct or indirect; (b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; (c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and (d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above, in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction.
"Tax Non-Compliance"	where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC's "Test for Tax Non-Compliance", as set out in Annex 1, where: (a) the "Economic Operator" means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause 4.3; and (b) any "Essential Subcontractor" means any Key Subcontractor.
"UK GDPR"	the UK General Data Protection Regulation, the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679);
"VAT"	value added tax as provided for in the Value Added Tax Act 1994.

2. Payment and Recovery of Sums Due

2.1 The Supplier shall invoice the Authority as specified in the Agreement. Without prejudice to the generality of the invoicing procedure specified in the Agreement, the Authority shall, before the start date of:

2.1.1 the initial Subscription Term; and

2.1.2 each renewal and/or extension of the Subscription Term,

create a Purchase Order (and generate a Purchase Order Number) for all fees payable for the Subscription Term and/or the renewal and/or extension to the Subscription Term (as the case may be) using the "*Ariba*" spend management solution (or such replacement spend management system agreed between the parties from time to time).

2.2 Provided that the Authority complies with clause 2.1, the Supplier: (a) shall not be permitted to raise its invoice without having first received the Purchase Order; and (b) acknowledges and agrees that should it commence Services without a Purchase Order Number:

2.2.1 the Supplier does so at its own risk; and

2.2.2 the Authority shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.

2.3 Each invoice and any Supporting Documentation required to be submitted in accordance with the invoicing procedure specified in the Agreement shall be submitted by the Supplier, as directed by the Authority from time to time via the Authority's electronic transaction system.

2.4 If any undisputed sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Authority in respect of any undisputed breach of the Agreement), that sum may be deducted by the Authority from any sum then due, or which may come due, to the Supplier under the Agreement.

3. Warranties

3.1 The Supplier represents and warrants that:

3.1.1 in the three years prior to the Effective Date, it has been in full compliance with all applicable securities and Laws related to Tax in the United Kingdom and in the jurisdiction in which it is established;

3.1.2 it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and

3.1.3 no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue and the Supplier has notified the Authority of any profit warnings issued in respect of the Supplier in the three years prior to the Effective Date.

3.2 If at any time the Supplier becomes aware that a representation or warranty given by it under Clause 3.1.1, 3.1.2 and/or 3.1.3 has been breached, is untrue, or is misleading, it shall immediately notify the Authority of the relevant occurrence in sufficient detail to enable the Authority to make an accurate assessment of the situation.

3.3 In the event that the warranty given by the Supplier pursuant to Clause 3.1.2 is materially untrue, the Authority shall be entitled to terminate the Agreement pursuant to the Call-Off clause which provides the

Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

4. Promoting Tax Compliance

4.1 All amounts stated are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.

4.2 To the extent applicable to the Supplier, the Supplier shall at all times comply with all Laws relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.

4.3 The Supplier shall provide to the Authority the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or Subcontractor of the Supplier prior to the provision of any material Services under the Agreement by that agent, supplier or Subcontractor. Upon a request by the Authority, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor supplying Services under the Agreement.

4.4 If, at any point during the Term, there is Tax Non-Compliance, the Supplier shall:

4.4.1 notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and

4.4.2 promptly provide to the Authority:

(a) details of the steps which the Supplier is taking to resolve the Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

(b) such other information in relation to the Tax Non-Compliance as the Authority may reasonably require.

4.5 The Supplier shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause 4.5 shall be paid in cleared funds by the Supplier to the Authority not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Authority.

4.6 Upon the Authority's request, the Supplier shall provide (promptly or within such other period notified by the Authority) information which demonstrates how the Supplier complies with its Tax obligations.

4.7 If the Supplier:

4.7.1 fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with Clauses 4.2, 4.4.1 and/or 4.6 this may be a material breach of the Agreement;

4.7.2 fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with a reasonable request by the Authority that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as

required by Clause 4.3 on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in Tax Non-Compliance this shall be a material breach of the Agreement; and/or

4.7.3 fails to provide details of steps being taken and mitigating factors pursuant to Clause 4.4.2 which in the reasonable opinion of the Authority are acceptable this shall be a material breach of the Agreement;

and any such material breach shall allow the Authority to terminate the Agreement pursuant to the CallOff Clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

4.8 The Authority may internally share any information which it receives under Clauses 4.3 to 4.4 (inclusive) and 4.6, for the purpose of the collection and management of revenue for which the Authority is responsible.

5. Use of Off-shore Tax Structures

5.1 Subject to the principles of non-discrimination against undertakings based either in member countries of the European Union or in signatory countries of the World Trade Organisation Agreement on Government Procurement, the Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place (unless otherwise agreed with the Authority) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description which would otherwise be payable by it or them on or in connection with the payments made by or on behalf of the Authority under or pursuant to this Agreement or (in the case of any Key Subcontractor and its Connected Companies) United Kingdom Tax which would be payable by it or them on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Key Subcontract (**"Prohibited Transactions"**). Prohibited Transactions shall not include transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties' business.

5.2 The Supplier shall notify the Authority in writing (with reasonable supporting detail) of any proposal for the Supplier or any of its Connected Companies, or for a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall notify the Authority within a reasonable time to allow the Authority to consider the proposed Prohibited Transaction before it is due to be put in place.

5.3 In the event of a Prohibited Transaction being entered into in breach of Clause 5.1 above, or in the event that circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Authority and, in order to ensure future compliance with the requirements of Clauses 5.1 and 5.2, the Parties (and the Supplier shall procure that the Key Subcontractor, where applicable) shall agree (at no cost to the Authority) timely and appropriate changes to any such arrangements by the undertakings concerned, resolving the matter (if required) through the escalation process in the Agreement.

5.4 Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Clauses 5.2 and 5.3 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

6 Data Protection and off-shoring

6.1 The parties agree that the Supplier shall, whether it is the Controller or Processor, in relation to any Personal Data processed in connection with its obligations under the Agreement:

6.1.1 not transfer Personal Data outside of the United Kingdom unless the following conditions are fulfilled:

(a) any transfer is made in accordance with the terms and conditions of the DPA;

(b) the Data Subject has enforceable rights and effective legal remedies as set out in the DPA;

(c) the Supplier or any applicable Processor complies with its obligations under the Data Protection Law by providing an appropriate level of protection to any Personal Data that is transferred (as set out in the DPA); and

(d) subject to section 3.1 of the DPA the Supplier or any applicable Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data.

6.2 The Authority retains the right to terminate the Agreement pursuant to the clause that provides the Authority the right to terminate the Agreement for Supplier's material breach of the Agreement (termination for Supplier cause or equivalent clause).

6.3 The Parties acknowledge and agree that: (a) the DPA applies to the Order Form; and (b) the Parties will, for a reasonable period following the date of the Order Form (not to exceed three (3) months from and including the effective date of the Order Form) continue to discuss the DPA and, if mutually agreed, document in writing amendments to the DPA.

7 Commissioners for Revenue and Customs Act 2005 and related Legislation

7.1 If, and to the extent, the Supplier (through its provision of the Service) accesses Authority Data that comprises revenue and customs information relating to a person acquired as a result of, or held in connection with, the exercise of a function of the Revenue and Customs (construed within the meanings of Sections 18 and 19 of the Commissioners for Revenue and Customs Act 2005 ("**CRCA**")) (the "**Customs Information**") then the Supplier shall comply with and shall ensure that all Supplier Personnel who will have access to, or are provided with, Customs Information comply with the obligations set out in Section 18 of the CRCA to maintain the confidentiality of Customs Information. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the aforesaid obligations may lead to a prosecution under Section 19 of CRCA.

7.2 If, and to the extent, the Supplier (through its provision of the Service) accesses Authority Data that comprises information relating to particular persons (construed within the meaning of Section 123 of the Social Security Administration Act 1992 ("**SSAA**")) (the "**Social Security Information**"), then the Supplier shall comply with and shall ensure that all Supplier Personnel who will have access to, or are provided with, Social Security Information comply with the obligations set out in Section 123 of the SSAA, which may apply to the fulfilment of some or all of the Services. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the Supplier's obligations under the SSAA may lead to a prosecution under that Act.

7.3 The Supplier shall regularly (not less than once every twelve (12 months) remind all Supplier Personnel who will have access to, or are provided with, Customs Information and/or Social Security Information in writing (which may include e-mail) of the obligations upon Supplier Personnel set out in Clause 7.1 above. The Supplier shall monitor the compliance by Supplier Personnel with such obligations.

7.4 The Supplier shall ensure that all Supplier Personnel who will have access to, or are provided with, Social Security Information and/or Customs Information have committed themselves to written obligations of confidentiality.

Annex 1

Excerpt from HMRC's "Test for Tax Non-Compliance"

Condition one (An in-scope entity or person)

1. There is a person or entity which is either: ("X")

1) The Economic Operator or Essential Subcontractor (EOS)
2) Part of the same Group of companies of EOS. An entity will be treated as within the same Group of EOS where that entities' financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts*[3];
3) Any director, shareholder or other person (P) which exercises control over EOS. 'Control' means P can secure, through holding of shares or powers under articles of association or other document that EOS's affairs are conducted in accordance with P's wishes.

Condition two (Arrangements involving evasion, abuse or tax avoidance)

2. X has been engaged in one or more of the following:

a. Fraudulent evasion[4];
b. Conduct caught by the General Anti-Abuse Rule[5];
c. Conduct caught by the Halifax Abuse principle[6];
d. Entered into arrangements caught by a DOTAS or VADR scheme[7];

[3] https://www.iasplus.com/en/standards/ifrs/ifrs10

[4] 'Fraudulent evasion' means any 'UK tax evasion offence' or 'UK tax evasion facilitation offence' as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.

[5] "General Anti-Abuse Rule" means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions

[6] "Halifax Abuse Principle" means the principle explained in the CJEU Case C-255/02 Halifax and others

[7] A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

e. Conduct caught by a recognised 'anti-avoidance rule' [8] being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or

where the arrangement is not effected for commercial purposes. 'Targeted Anti-Avoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;

f. Entered into an avoidance scheme identified by HMRC's published Spotlights list[9];

g. Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))

3. X's activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:

1. In respect of (a), either X:
    1. Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure[10]; or,
    2. Has been charged with an offence of fraudulent evasion.
2. In respect of (b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.
3. In respect of (b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.
4. In respect of (f) this condition is satisfied without any further steps being taken.
5. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

[8] The full definition of 'Anti-avoidance rule' can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly.

[9] Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: https://www.gov.uk/government/collections/tax-avoidance-schemescurrently-in-the-spotlight

[10] The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed.

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

1. DEFINITIONS

1.1. "**Affiliate**" means any legal entity in which SAP SE or Customer, directly or indirectly, holds more than 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 the agreement as defined in the applicable Order Form.

1.3. "**Authorized User**" means any individual to whom Customer grants access authorization to use the Cloud Service that is an employee, agent, contractor or representative of Customer, Customer's Affiliates, or 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 and its Affiliates.

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. "**Confidential Information**" means all information which the disclosing party protects against unrestricted disclosure to others that the disclosing party or its representatives designates as confidential, internal and/or proprietary at the time of disclosure, should reasonably be understood to be confidential at the time of disclosure given the nature of the information and the circumstances surrounding its disclosure.

1.7. "**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.

1.8. "**Documentation**" means SAP's then-current technical and functional documentation, including any roles and responsibilities descriptions relating to the Cloud Services which SAP makes available to Customer under the Agreement.

1.9. "**Export Laws**" means all applicable import, export control and sanctions laws, including without limitation, the laws of the United States, the EU, and Germany.

1.10. "**Feedback**" means input, comments or suggestions regarding SAP's business and technology direction, and the possible creation, modification, correction, improvement or enhancement of the Cloud Service.

1.11. "**Intellectual Property Rights**" means patents of any type, design rights, utility models or other similar invention rights, copyrights and related rights, trade secret, know-how or confidentiality rights, trademarks, trade names and service marks and any other intangible property rights, whether registered or unregistered, including applications (or rights to apply) and registrations for any of the foregoing, in any country, arising under statutory or common law or by contract and whether or not perfected, now existing or hereafter filed, issued, or acquired.

1.12. "**Order Form**" means the ordering document for a Cloud Service and/or Professional Services that references the GTC.

1.13. "**Professional Services**" means implementation services, consulting services or other related services provided under an Order Form and may also be referred to in the Agreement as "Consulting Services".

1.14. "**Representatives**" means a party's Affiliates, employees, contractors, sub-contractors, legal representatives, accountants, or other professional advisors.

1.15. "**SAP Materials**" means any materials (including statistical reports) provided, developed or made available by

SAP (independently or with Customer's cooperation) in the course of performance under the Agreement, including in the delivery of any support or Professional Services to Customer. SAP Materials do not include the Customer Data, Customer Confidential Information or the Cloud Service. SAP Materials may also be referred to in the Agreement as "Cloud Materials".

1.16. "**SAP SE**" means SAP SE, the parent company of SAP.

1.17. "**Subscription Term**" means the initial subscription term and if applicable any renewal subscription term of a Cloud Service identified in the Order Form.

1.18. "**Taxes**" means all transactional taxes, levies and similar charges (and any related interest and penalties) such as federal, state or local sales tax, value added tax, goods and services tax, use tax, property tax, excise tax, service tax or similar taxes.

1.19. "**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.

2. USAGE RIGHTS AND RESTRICTIONS

2.1. Grant of Rights

SAP grants to Customer a non-exclusive and non-transferable right to use the Cloud Service (including its implementation and configuration), SAP Materials and Documentation solely for Customer's and its Affiliates' internal business operations. Customer may use the Cloud Service world-wide, except Customer shall not use the Cloud Service from countries where such use is prohibited by Export Laws. Permitted uses and restrictions of the Cloud Service also apply to SAP 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. 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.

2.4. Suspension of Cloud Service

SAP may suspend or limit 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 or limitation. SAP will limit a suspension or limitation in time and scope as reasonably possible under the circumstances.

2.5. 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. SAP is not responsible for the content of these third party web services.

2.6. Mobile Access to Cloud Service

Authorized Users may access certain Cloud Services through mobile applications obtained from third-party websites such as Android or Apple app stores. The use of mobile applications may be governed by the terms and conditions presented upon download/access to the mobile application and not by the terms of the Agreement.

2.7. On-Premise Components

The Cloud Service may include on-premise components that can be downloaded and installed (including updates) by Customer. The System Availability SLA does not apply to these components. Customer may only use the on-premise components during the Subscription Term.

3. SAP RESPONSIBILITIES

3.1. Provisioning

SAP provides access to the Cloud Service as described in the Agreement. SAP makes the Cloud Service available and is responsible for its operation.

3.2. Support

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

3.3. Security

SAP will implement and maintain appropriate technical and organizational measures to protect the personal data processed by SAP as part of the Cloud Service as described in the Data Processing Agreement incorporated into the Order Form in compliance with applicable data protection law.

3.4. Modifications

3.4.1. Scope

3.4.1.1. As the Cloud Service evolves, SAP may improve or modify the Cloud Service (including support services, Maintenance Windows and Major Upgrade Windows). This includes the option to remove functionality from the Cloud Service where SAP either provides a functional equivalent or where this does not materially reduce functionality of the Cloud Service. Functionality beyond the initial scope of the Cloud Service may be subject to additional terms and Customer's use of such additional functionality shall be subject to those terms.

3.4.2. Modification Notices

3.4.2.1. SAP shall inform Customer of modifications to the Cloud Service within a reasonable period in advance. SAP shall provide Customer one (1) month's advance notice before changing its Maintenance and Major Upgrade Windows (unless such change is a reduction in the duration of the applicable Maintenance or Major Upgrade Windows) and support services.

3.4.2.2. Where in justified cases, SAP removes functionality from the Cloud Service without providing a functional equivalent, SAP shall provide Customer six (6) months' advance notice.

3.4.3. Customer Termination

If a modification materially degrades the overall functionality of the affected Cloud Service, Customer may terminate its subscription to the affected Cloud Service by providing written notice to SAP within one (1) month of SAP's applicable notice. If SAP does not receive timely notice, Customer is deemed to have accepted the modification.

4. CUSTOMER AND PERSONAL DATA

4.1. Customer Ownership

Customer retains all rights in and related to the Customer Data. SAP may use Customer-provided trademarks solely to provide and support the Cloud Service.

4.2. 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 non-exclusive right to process and use Customer Data to provide and support the Cloud Service and as set out in the Agreement.

4.3. Personal Data

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

4.4. Security

Customer will maintain reasonable security standards for its Authorized Users' use of the Cloud Service. Customer will not conduct or authorize penetration tests of the Cloud Service without written advance approval from SAP.

4.5. Access to Customer Data

4.5.1. 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.

4.5.2. 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.

4.5.3. 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.

4.5.4. 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 shall pay fees as stated in the Order Form. If Customer does not pay fees in accordance with the terms of the Agreement then, in addition to any other available remedies, SAP may suspend Customer's use of the applicable Cloud Service until payment of all outstanding fees is made. SAP shall provide Customer with prior written notice before any such suspension. Any fees not paid when due shall accrue interest at the maximum legal rate. Purchase orders are for administrative convenience only. SAP may issue an invoice and collect payment without a corresponding purchase order. Customer may not withhold, reduce or set-off fees owed. Customer may not reduce Usage Metrics during the Subscription Term. All Order Forms are noncancellable. All fees are non-refundable except per Sections 6.3 or 7.4.2.

5.2. Taxes

All fees and other charges are subject to applicable Taxes, which will be charged in addition to fees under the Agreement.

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 (30) days' prior written notice of the other party's material breach of any provision of the Agreement (including Customer's failure to pay any money due hereunder within thirty (30) days of the payment due date) unless the breaching party has cured the breach during such thirty (30) day period;

b) as permitted under Sections 3.4.3, 7.3.b), 7.4.3, 8.1.4, or 13.4 (with termination effective thirty (30) 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 13.6.

6.3. Refund and Payments

For termination by Customer or termination under Sections 8.1.4 or 13.4 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 (unless such refund is prohibited by Export Laws); 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 retained, returned, or destroyed as required by the Agreement or applicable law; 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, 12 and 13 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) correction of the deficient Cloud Service; and

b) if SAP fails to correct the deficient Cloud Service, Customer may terminate its subscription for the affected Cloud Service. Any termination must occur within three (3) months of SAP's failure to correct the deficient Cloud Service.

7.4. System Availability

7.1.1. 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").

7.1.2. 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.

7.1.3. In the event SAP fails to meet the SLA (i) for four (4) consecutive months, or (ii) for five (5) or more months during any twelve (12) month period, or (iii) at a system availability level of at least 95% for one (1) calendar month, Customer may terminate its subscriptions for the affected Cloud Service by providing SAP with written notice within thirty (30) 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, and SAP and its subcontractors disclaim all representations, warranties, terms, conditions or statements, which might have effect between the parties or be implied or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded to the fullest extent permitted by law including the implied conditions, warranties or other terms as to quality, suitability, originality, or fitness for a particular use or purpose. Further, except as expressly provided in this Agreement, neither SAP nor its subcontractors make any representations, warranties, terms, conditions or statements of 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

8.1.1. 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 belonging to such third party. 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.

8.1.2. SAP's obligations under Section 8.1 will not apply if the claim results from:

a) use of the Cloud Service in conjunction with any product or service not provided by SAP;

b) use of the Cloud Service provided for no fee;

c) Customer's failure to timely notify SAP in writing of any such claim if SAP is prejudiced by Customer's failure to provide or delay in providing such notice; or

d) any use of the Cloud Service not permitted under the Agreement.

8.1.3. If a third party makes a claim or in SAP's reasonable opinion is likely to make such a claim, SAP may at its sole option and expense:

a) procure for Customer the right to continue using the Cloud Service under the terms of the Agreement; or

b) replace or modify the Cloud Service to be non-infringing without a material decrease in functionality.

8.1.4. 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.

8.1.5. SAP expressly reserves the right to cease such defense of any claim(s) if the applicable Cloud Service is no longer alleged to infringe or misappropriate the third party's rights.

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

All third party claims under Section 8 shall be conducted as follows:

a) The party against whom a third party claim is brought (the "**Named Party**") will timely notify the other party (the "**Defending Party**") in writing of any claim. The Named Party shall reasonably cooperate in the defense and may appear (at its own expense) through counsel reasonably acceptable to the Defending Party subject to Section 8.3b).

b) The Defending Party 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 Named Party.

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. No Cap on Liability

9.1.1. Subject to Section 9.3 neither party's liability is capped for damages resulting from:

a) the parties' obligations under Section 8.1.1 and 8.2 (excluding SAP's obligation under Section 8.1.1 where the third party claim(s) relates to Cloud Services not developed by SAP);

b) Customer's unauthorized use of any Cloud Service and / or any failure by Customer to pay any fees due under the Agreement;

c) Breach of the obligations imposed by s.12 Sales of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982; and/or

d) Any liability for other losses which cannot be excluded or limited by applicable law.

9.1.2. Neither party's liability is capped for damages resulting from:

a) fraud or fraudulent misrepresentation,

b) death or bodily injury arising from either party's negligence.

9.2. Liability Cap

Except as set forth in Section 9.1.1 and 9.3, and regardless of the basis of liability (whether arising out of liability under breach of contract, tort (including but not limited to negligence) misrepresentation or breach of statutory duty, breach of warranty, claims by third parties arising from any breach of this Agreement) the maximum aggregate liability of either party (or its respective Affiliates or SAP's subcontractors) arising out of or accruing under or in connection with the Agreement to the other or to any other person or entity for all events (or series of connected events) arising in any twelve (12) month period will not exceed the annual subscription fees paid for the applicable Cloud Service associated with the damages for that twelve (12) month period. Any "twelve (12) month period" commences on the Subscription Term start date or any of its yearly anniversaries.

9.3. Exclusion of Damages

To the extent permitted by law in no case will:

a) either party (or its respective Affiliates or SAP's subcontractors) be liable to the other party for

(i) any special, incidental, consequential, or indirect damages, or

(ii)the following damages: loss of goodwill or business profits, losses resulting from work stoppage, loss of revenue or opportunity; in each case (whether such losses are direct or indirect) or

(iii) exemplary or punitive damages; and

b) SAP be liable for any damages caused by any Cloud Service provided for no fee.

9.4. The Agreement allocates the risk between SAP and the Customer. The fees for the Cloud Services and / or Professional Services reflects this allocation of risk and limitation of liability.

10. INTELLECTUAL PROPERTY RIGHTS

10.1. SAP Ownership

10.1.1. Except for any rights expressly granted to Customer under the Agreement, SAP, SAP SE, their Affiliates or licensors own all Intellectual Property Rights in and derivative works of: a) the Cloud Service;

b) SAP Materials;

c) Documentation; and

d) any Professional Services, design contributions, related knowledge or processes, whether or not developed for Customer.

10.1.2. Customer shall execute such documentation and take such other steps as is reasonably necessary to secure SAP's or SAP SE's title over such rights.

10.2. Acceptable Use Policy

10.2.1. With respect to the Cloud Service, Customer will not:

a) Except to the extent such rights cannot be validly waived by law, copy, translate, disassemble, decompile, make derivative works, or reverse engineer the Cloud Service or SAP Materials (or attempt any of the foregoing);

b) enter, store, or transfer any content or data on or via the Cloud Service that is unlawful or infringes any Intellectual Property Rights;

c) circumvent or endanger the operation or security of the Cloud Service; or

d) remove SAP's copyright and authorship notices.

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 Professional Services.

11. CONFIDENTIALITY

11.1. Use of Confidential Information

11.1.1. The receiving party shall:

a) maintain all Confidential Information of the disclosing party in strict confidence, taking steps to protect the disclosing party's Confidential Information substantially similar to those steps that the receiving party takes to protect its own Confidential Information, which shall not be less than a reasonable standard of care;

b) not disclose or reveal any Confidential Information of the disclosing party to any person other than its Representatives 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;

c) not use or reproduce any Confidential Information of the disclosing party for any purpose outside the scope of the Agreement; and

d) retain any and all confidential, internal, or proprietary notices or legends which appear on the original and on any reproductions.

11.1.2. Customer shall not disclose any information about the Agreement, its terms and conditions, the pricing or any other related facts to any third party.

11.1.3. Confidential Information of either party disclosed prior to execution of the Agreement will be subject to Section

11.

11.2. Compelled Disclosure

The receiving party may disclose the disclosing party's Confidential Information to the extent required by law, regulation, court order or regulatory agency; provided, that the receiving party required to make such a disclosure uses reasonable efforts to give the disclosing party reasonable prior notice of such required disclosure (to the extent legally permitted) and provides reasonable assistance in contesting the required disclosure, at the request and cost of the disclosing party. The receiving party and its Representatives shall use commercially reasonable efforts to disclose only that portion of the Confidential Information which is legally requested to be disclosed and shall request that all Confidential Information that is so disclosed is accorded confidential treatment.

11.3. 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) has become generally known or available to the public through no act or omission by the receiving party;

c) at the time of disclosure, was known to the receiving party free of confidentiality restrictions;

d) is lawfully acquired free of restriction by the receiving party from a third party having the right to furnish such Confidential Information; or

e) the disclosing party agrees in writing is free of confidentiality restrictions.

11.4. Destruction and Return of Confidential Information

Upon the disclosing party's request, the receiving party shall promptly destroy or return the disclosing party's Confidential Information, including copies and reproductions of it. The obligation to destroy or return Confidential Information shall not apply:

a) if legal proceedings related to the Confidential Information prohibit its return or destruction, until the proceedings are settled or a final judgment is rendered;

b) to Confidential Information held in archive or back-up systems under general systems archiving or backup policies and which is not generally accessible to the personnel of the receiving party; or

c) to Confidential Information the receiving party is legally entitled or required to retain.

12. FEEDBACK

12.1. Customer may at its sole discretion and option provide SAP with Feedback. In such instance, SAP, SAP SE and its Affiliates may in their sole discretion retain and freely use, incorporate or otherwise exploit such Feedback without restriction, compensation or attribution to the source of the Feedback.

13. MISCELLANEOUS

13.1. Severability

If any provision of the Agreement is held to be wholly or in part invalid or unenforceable, the invalidity or unenforceability will not affect the other provisions of the Agreement and this Agreement shall be construed as if such invalid or unenforceable provision had never been contained herein. 13.2. No Waiver

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

13.3. Counterparts

The Agreement may be signed in counterparts, each of which is an original and together constitute one Agreement. Electronic signatures via DocuSign or any other form as determined by SAP are deemed original signatures.

13.4. Trade Compliance

13.1.1. SAP and Customer shall comply with Export Laws in the performance of this Agreement. SAP Confidential Information is subject to Export Laws. Customer, its Affiliates, and Authorized Users shall not directly or indirectly export, re-export, release, or transfer Confidential Information in violation of Export Laws. Customer is solely responsible for compliance with Export Laws related to Customer Data, including obtaining any required export authorizations for Customer Data. Customer shall not use the Cloud Service from the following list of countries which may be updated from time to time: Crimea/Sevastopol, Cuba, Iran, the People's Republic of Korea (North Korea) or Syria.

13.1.2. Upon SAP's request, Customer shall provide information and documents to support obtaining an export authorization. Upon written notice to Customer SAP may immediately terminate Customer's subscription to the affected Cloud Service if:

a) the competent authority does not grant such export authorization within 18 months; or

b) Export Laws prohibit SAP from providing the Cloud Service or Professional Services to Customer.

13.5. Notices

All notices will be in writing and given when delivered to the address set forth in an Order Form. Notices from SAP to Customer may be in the form of an electronic notice to Customer's authorized representative or administrator. SAP may provide notice of modifications to the Cloud Service under Section 3.4.2 via Documentation, release notes or publication. System notifications and information from SAP relating to the operation, hosting or support of the Cloud Service can also be provided within the Cloud Service, or made available via the SAP Support Portal.

13.6. Assignment

Without SAP's prior written consent, Customer may not assign, delegate or otherwise 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

13.7. Subcontracting

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

13.8. 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.

13.9. 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.

13.10. Governing Law

The Agreement and any claims (including any non-contractual claims) arising out of or in connection with this Agreement and its subject matter will be governed by and construed under the laws of England and Wales. The United Nations Convention on Contracts for the International Sale of Goods and any conflicts of law principles and the Uniform Computer Information Transactions Act (where enacted) will not apply to the Agreement.

13.11. Jurisdiction and Mandatory Venue

The parties submit to the exclusive jurisdiction of the courts located in London. The parties waive any objections to the venue or jurisdictions identified in this provision.

13.12. Statute of Limitation

Either party must initiate a cause of action for any claim(s) relating to the Agreement and its subject matter within 1 year from the date when the party knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

13.13. 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 Agreement and the parties disclaim any reliance on them. Each party acknowledges that (i) in entering into this Agreement it has not relied on any representation, discussion, collateral contract or other assurance except those set out in this Agreement and hereby waives all rights and remedies which, but for this section, might otherwise be available to it in respect of any such representation, discussion, collateral contract or other assurance and (ii) it shall have no remedies in respect of any representation or warranty that is not expressly set out in this Agreement. The Agreement may be modified solely in writing signed by both parties, except as permitted under the Agreement. Terms and conditions of any Customerissued purchase order shall have no force and effect, even if SAP accepts or does not otherwise reject the purchase order. Nothing in this Agreement shall limit or exclude any liability for fraud.

13.14. Contracts (Rights of Third Parties) Act 1999.

Notwithstanding any other provision in this Agreement, nothing in this Agreement shall create or confer (whether expressly or by implication) any rights or other benefits whether pursuant to the (Contracts Rights of Third Parties) Act 1999 or otherwise in favour of any person not a party hereto.