Master Cloud Customer Agreement

Between **SAP America, Inc.**
3999 West Chester Pike
Newtown Square Pennsylvania, 19073
United States
("SAP")

And **Sample Co**
123 First Street
Anywhere, 000000
United States
("Customer")

Case ID: 123456789

1. DEFINITIONS

"**Order Form**" means any mutually agreed ordering document issued by SAP that references the MCCA.

"**MCCA**" or Master Cloud Customer Agreement means this document including the Schedules referenced in Section 3.

Capitalized terms shall have the meaning ascribed to them in this MCCA or in an Order Form.

2. EFFECTIVE DATE

The MCCA shall become effective when signed or accepted by Customer and received by SAP ("**Effective Date**").

3. REFERENCED DOCUMENTS

3.1. The following documents shall apply in the order of precedence as follows:

- Order Form
- Master Cloud Customer Agreement
- Schedule 1 - Support Schedule for Cloud Services ("**Support Schedule**")
- Schedule 2 - Service Level Agreement for Cloud Services ("**SLA**")
- Schedule 3 - Data Processing Agreement for Cloud Services, SAP Support and SAP Services ("**DPA**")
- Schedule 4 - Security Measures for Cloud Services ("**Security Measures**")
- Schedule 5 - Product Development Schedule
- Schedule 6 - SAP AI Terms
- Schedule 7 - Professional Services Schedule
- Schedule 8 - General Terms and Conditions for Cloud Services ("**GTC**")

3.2. The above Schedules are attached as of the Effective Date and are an integral part of the MCCA. SAP can update these Schedules where and as permitted in the respective Schedule.

4. ORDER

4.1. This MCCA establishes the contractual framework under which the parties may enter into an Order Form. An Order Form will detail the specific terms related to the transaction.

4.2. Any contract previously executed by the parties remains unaffected unless the parties expressly agree to apply the MCCA.

Accepted By:

Sample Co.
(Customer)

Name:

Title:

Data:

Schedule 1

SUPPORT SCHEDULE FOR CLOUD SERVICES

This Support Schedule is part of the Agreement for Cloud Services between SAP and Customer.

1. DEFINITIONS

1.1. "**Go-Live**" marks the point in time from when, after set-up of the Cloud Services for Customer, the Cloud Services can be used by Customer for processing real data in live operation mode and for running Customer's internal business operations in accordance with its agreement for such Cloud Services.

1.2. "**Local Business Hours**" means 8 a.m. (08:00) to 6 p.m. (18:00) Monday to Friday excluding local holidays, in accordance with local time zone applicable to the Customer's address.

1.3. "**SAP's Customer Support Website**" means SAP's customer facing support website (see: https://support.sap.com unless a different support website is listed in the Agreement or https://support.sap.com/contactus). In selected Cloud Services, support can also be accessed via the application itself.

2. SCOPE OF SUPPORT AND SUCCESS OFFERINGS

2.1. General

2.1.1. SAP offers the following:

(a) SAP Enterprise Support, cloud editions: Foundational engagement support as part of the Cloud Service with focus on customer interaction and case resolution.

(b) 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.

(c) SAP Enterprise Support, cloud editions is included in the subscription fees for the Cloud Services stated in the Order Form unless alternative support terms are agreed. SAP Preferred Success may be purchased for eligible Cloud Services for an additional fee, as an add-on to SAP Enterprise Support, cloud editions. SAP Preferred Success is not available, and not provided, for any third-party cloud services purchased through SAP.

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

2.1.3. Customer Interaction Center languages: SAP provides initial telephone contact for Customer Contacts through the SAP one support phone number "CALL-1-SAP" (see CALL-1-SAP page: https://support.sap.com/contactus) or via other solution specific hotlines in the following languages: English (24x7) 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 or third party support engineers worldwide are handled in English only.

2.2. Mission Critical Support

Feature	SAP Enterprise Support, cloud editions	SAP Preferred Success
24x7 mission critical support for P1 and P2 cases (English only)	Global case handling by SAP for issues related to support, including Service Level Agreements for Initial Response, Ongoing Communications and Corrective Action Targets (as set forth in Section 3 below).	24x7 prioritized case handling and enhanced Initial Response and Corrective Action Targets (as set forth in Section 3 below).
Non-mission critical	Available during Local Business Hours(as	Enhanced Initial Response Targets (as

support for P3 and P4 cases (English only)	set forth in Section 3 below).	set forth in Section 3 below).

Feature	SAP Enterprise Support, cloud editions	SAP Preferred Success
24x7 Customer interaction center	Support center that customers may contact for general support related inquiries through the contact channels described in Section 2.1.3.	Delivered as part of SAP Enterprise Support, cloud editions.
Global support backbone	SAP's knowledge database and extranet where SAP makes available content and services to customers and partners of SAP only. This includes SAP's Customer Support Website.	
End-to-end supportability	Support for cases that occur in integrated business scenarios consisting of SAP Cloud Services or both SAP Cloud Services and SAP Software with a valid SAP support agreement.	

2.3. Learning and Empowerment

Feature	SAP Enterprise Support, cloud editions	SAP Preferred Success
Remote SAP support content and services	Remote support content and services (e.g., Meet-the-Expert sessions) in various formats which may include live and recorded webinars, tutorials, best practices, self-paced learning materials and workshop-style interactive remote sessions. Content and session schedules are stated on SAP's Customer Support Website in the SAP Enterprise Support Academy section. Scheduling, availability and delivery methodology is at SAP's discretion.	Access to demo systems, live sessions with instructors, examinations and certifications specific to the Cloud Service for up to 5 Customer Contacts. SAP Preferred Success exclusive learning content related to the Cloud Service in various formats which may include live and recorded webinars, best practices, and workshop-style interactive remote sessions. Scheduling, availability and delivery methodology is at SAP's discretion.
Release update information	Generally available documented summaries, webinars and videos provided by SAP to inform and instruct customers on new product release changes. Self-service through web and community.	Release guidance specific to the Cloud Service.

2.4. Collaboration

Feature	SAP Enterprise Support, cloud editions	SAP Preferred Success
SAP support advisory services	Access to experts who help customers with support-related requests and advise on the appropriate SAP Enterprise Support content and services for their needs.	Delivered as part of SAP Enterprise Support, cloud editions.
Support via chat	Available during business hours in English language for non-Mission Critical Support	

	issues, where available for the Cloud Service.	

Feature	SAP Enterprise Support, cloud editions	SAP Preferred Success
Support via web and platform for social business collaboration	Access to SAP's Customer Support Website, including social media-based empowerment and collaboration, with peers and SAP experts.	Access to exclusive SAP Preferred Success collaboration platform.
Support and success reporting	SAP Enterprise Support reporting: A report or dashboard analyzing and documenting the status of support services and achievements hereunder.	Reports, dashboards, or other reporting components and capabilities regarding the overall engagement, full customer lifecycle, and productive use of the solution, including relevant feature adoption, technical and product usage and status of support services and achievements hereunder, specific to the Cloud Service.
Preferred Success resources and guidance		Access to success resources to provide guidance on onboarding, product adoption and usage, best practices and operational excellence. This may include a customer success partner as the primary contact for ongoing success management, success planning, technical guidance and mentorship, and support case oversight throughout the Customer lifecycle. Assignment of a customer success partner is at SAP's discretion.
Regular checkpoint		Periodic review of Cloud Service, success plan, critical issues, reporting and best practices. May include in-person delivery, at SAP's discretion.
Success Plan		A success plan outlines steps towards achieving key business milestones and objectives throughout the customer lifecycle. Focus topics include challenges, consumption, adoption and cycle planning.

2.5. Innovation and Value Realization

Feature	SAP Enterprise Support, cloud editions	SAP Preferred Success
Proactive checks proposed by SAP	Support services, providing recommendations for the specific customer situation. Such services are delivered remotely upon Customer request.	Expert-led checks, providing recommendations based on SAP best practices or recommended configuration(s).
Product roadmaps	Self-service through web.	Delivered as part of SAP Enterprise Support, cloud editions.

Refresh of test instance	Self-service or request through web for initiating the refresh as offered and required by respective solution.	Access to SAP assistance with managing the refreshing of test instances up to 2 times per year, where applicable.

2.6. Application Lifecycle Management

Feature	**SAP Enterprise Support, cloud editions**	**SAP Preferred Success**
Application lifecycle management ("**ALM**")	Software or online services for application lifecycle management made available by SAP. Feature scope and availability details are set forth on SAP's Customer Support Website (see: https://support.sap.com/en/alm) and usage rights (see: https://support.sap.com/en/alm/usage-rights).	Delivered as part of SAP Enterprise Support, cloud editions.

3. CUSTOMER RESPONSE LEVELS

3.1. SAP responds to submitted support cases as described in the table below.

Priority	**Definition**	**Response Level**
P1	Very High A case 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) a productive service is completely down; (b) the imminent system Go-Live or upgrade of a production system cannot be completed; (c) the customer's core business processes are seriously affected A workaround is not available for each circumstance. The case requires immediate processing because the malfunction may cause serious losses.	Initial Response: Within 1 hour of case submission. Ongoing Communication: Unless otherwise communicated by SAP, once every hour. Corrective Action Target: SAP to provide for cases either a resolution; or workaround; or action plan within 4 hours.
P2	High A case 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 case is to be processed as quickly as possible because a continuing malfunction can seriously disrupt the entire productive business flow.	Initial Response: Within 4 hours of case submission for SAP Enterprise Support, cloud edition customers and within 2 hours of case submission for SAP Preferred Success customers. Ongoing Communication: Unless otherwise communicated by SAP, once every 6 hours. Corrective Action Target: SAP to provide for cases either a resolution; or workaround; or action plan within 3 business days for SAP Preferred Success

Priority	Definition	Response Level
		customers only.
P3	Medium A case 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 1 business day of case submission for SAP Enterprise Support, cloud edition customers, and within 4 business hours of case being received for SAP Preferred Success customers. Ongoing Communication: Unless otherwise communicated by SAP, once every 3 business days for non-defect Issues and 10 business days for product defect issues. A non-defect issue is a reported support case that does not involve a defect in the applicable Cloud Service and does not require engineering, development or operations personnel to resolve.
P4	Low A case 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 2 business days of case submission for SAP Enterprise Support, cloud editions customers and within 1 business day of case submission for SAP Preferred Success customers. Ongoing Communication: Unless otherwise communicated by SAP, once every week.

3.2. The following types of cases are excluded from customer response levels as described above:

(a) cases regarding a release, version or functionalities of Cloud Services developed specially for Customer (including those developed by SAP Custom Development or by SAP subsidiaries or individual content services);

(b) the root cause behind the case is not a malfunction but missing functionality (development request);

(c) the case is a consulting or how-to request.

4. CUSTOMER RESPONSIBILITIES

4.1. Customer Contact

4.1.1. Customer shall designate at least 2 and up to 5 qualified English-speaking contact persons per Cloud Service (each a "**Customer Contact**"). Customer Contacts include designated support contact, authorized support contact, key user, application administrator or system administrators whose roles within specific Cloud Services are authorized to contact or access the Customer Interaction Center, SAP Support Advisory Services and Mission Critical Support services.

4.1.2. The Customer Contact is responsible for managing all business-related tasks of the Cloud Service related to Customer's business, such as:

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

(b) manage background jobs and the distribution of business tasks across users (if available);

(c) manage and monitor connections to Customer's third-party systems (if available);

(d) support the adoption of the Cloud Service.

4.2. Contact Details

Customer will provide contact details (in particular, e-mail address and telephone number) by 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 a Cloud Service through SAP's Customer Support Website. Only authorized Customer Contacts may contact SAP's support organization.

4.3. Cooperation

Customer Contact shall reasonably cooperate with SAP to resolve support cases,and will have adequate technical expertise and knowledge of its configuration of the Cloud Services to provide relevant information to enable SAP to reproduce, troubleshoot and resolve the experienced error.

Schedule 2

SERVICE LEVEL AGREEMENT FOR CLOUD SERVICES

1. DEFINITIONS

1.1. "**Credit**" means 2% of the Monthly Subscription Fees for the affected subscription-based Cloud Service or the monthly Cloud Credits (as defined in the Order Form) consumed for the affected consumption-based Cloud Service, for each 1% below the System Availability SLA, not to exceed 100% of the fees paid or Cloud Credit consumed by the Customer for the relevant Month for the affected Cloud Service.

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 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 on 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 on 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:

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

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 per week during a Month.

1.11. "**UTC**" means Coordinated Universal Time standard is 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 for 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 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 is available.

3. CHANGES TO WINDOWS

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

Schedule 3

DATA PROCESSING AGREEMENT FOR CLOUD SERVICES, SAP SUPPORT AND SAP SERVICES ("DPA")

1. DEFINITIONS

1.1. "**Cloud Service**" means any distinct, hosted, supported and operated on-demand solution as set out in the Agreement.

1.2. "**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 processing of Personal Data.

1.3. "**Data Protection Law**" means the applicable legislation protecting the fundamental rights and freedoms of natural persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

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

1.5. "**EU Standard Contractual Clauses**" means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof which will automatically apply.

1.6. "**GDPR**" means the General Data Protection Regulation (EU) 2016/679.

1.7. "**List of Subprocessors**" means a list of the name, address and role of each Subprocessor SAP uses to provide SAP Services.

1.8. "**My Trust Center**" means information available on the SAP support portal (see: https://support.sap.com/en/my-support/trust-center.html) or any subsequent website(s) made available by SAP to Customer.

1.9. "**Personal Data**" means any information relating to a Data Subject. For the purposes of Cloud Services, Personal Data is a sub-set of Customer Data (as defined in the Agreement).

1.10. "**Personal Data Breach**" means a confirmed breach of SAP's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data for which a Processor is required under Data Protection Law to provide notice to the Controller.

1.11. "**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.

1.12. "**Professional Services**" means implementation services, consulting services and/or other related services as set out in the Agreement and may also be referred to in the Agreement as "Consulting Services" or "Services".

1.13. **"SAP Services"** means Cloud Services, Professional Services or SAP Support as set out in the Agreement.

1.14. **"SAP Support"** means SAP support services as set out in the Agreement.

1.15. **"Subprocessor"** or **"sub-processor"** means SAP's Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP, SAP SE or SAP SE's Affiliates in connection with SAP Services to process Personal Data under this DPA.

1.16. **"Technical and Organizational Measures"** means the following: (a) for Cloud Services, the technical and organizational measures described in the Security Measures for the relevant Cloud Service; and (b) for SAP Support and Professional Services, the technical and organizational measures for SAP Support and Professional Services (each currently published here: https://www.sap.com/about/trust-center/agreements.html).

1.17. "**Third Country**" means any country, organization or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.

2. BACKGROUND

2.1. Scope

2.1.1. This DPA is incorporated into and forms part of the Agreement between SAP and Customer and sets forth the terms and conditions related to the processing of Personal Data by SAP and its Subprocessors in connection with delivering SAP Services.

2.1.2. This DPA applies only to Personal Data which is processed by SAP or its Subprocessors on behalf of the Customer as part of providing SAP Services.

2.1.3. Where SAP or a Subprocessor makes available non-production environments of SAP Services, Customer shall not store Personal Data in such environments. Non-production environments are not intended for the processing and storage of Personal Data and are excluded from the scope of this DPA.

2.2. Structure

Schedules 1 and 2 are incorporated into 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.

2.3. Governance

2.3.1. SAP acts as a Processor under this DPA. Customer and those entities that Customer authorizes to use SAP Services under the Agreement act as a Controller or Processor. For the purposes of this DPA, where Customer acts as Processor, it does so under the instructions of its Controller(s).

2.3.2. Customer acts as a single point of contact and shall obtain any relevant authorizations, consents, instructions and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable, approval to use SAP as a Processor. Where authorizations, consents, instructions and permissions are provided by Customer, these are provided not only on behalf of the Customer but also on behalf of any other Controller. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use SAP Services. Customer shall forward such information and notices to the relevant Controllers.

3. SECURITY OF PROCESSING

3.1. Technical and Organizational Measures

SAP has implemented and will apply the Technical and Organizational Measures. Customer has reviewed the appropriateness of such measures before it executes an Agreement that incorporates this DPA.

3.2. Changes

3.2.1. SAP applies the Technical and Organizational Measures to SAP's entire customer base hosted out of the same data center or receiving the same SAP Services. SAP will review and may change the Technical and Organizational Measures at any time without prior notice so long as such changes maintain an overall level of security for Personal Data that is comparable or better and is not diminished. For example, new measures may be added or individual measures may be replaced by new measures that serve the same purpose. SAP will publish such updated versions of Technical and Organizational Measures on My Trust Center and where available Customer may subscribe to receive e-mail notification of updated versions.

4. OBLIGATIONS

4.1. Instructions from Customer

SAP will process Personal Data only in accordance with documented instructions from Customer. In entering into the Agreement and by using the SAP Service, Customer instructs SAP to process Personal Data to provide and support the SAP Service as set out in the Agreement (including this DPA). SAP will use reasonable efforts to follow any other Customer instructions, as long as they are technically feasible, do not require changes to the SAP Service and are in accordance with Data Protection Law. If SAP cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will notify Customer (e-mail permitted) without undue delay.

4.2. 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.

4.3. 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.

4.4. Data Subject Requests and Cooperation

4.4.1. SAP shall provide functionality for production systems of the Cloud Service that supports Customer's ability to correct, delete or anonymize Personal Data from a Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided as part of the production systems of the Cloud Service, SAP will correct, delete or anonymize any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

4.4.2. 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. If SAP receives a request from a Data Subject in relation to the Personal Data processed hereunder, SAP will promptly notify Customer (where the Data Subject has provided information to identify the Customer) via e-mail and shall not respond to such request itself but instead ask the Data Subject to redirect its request to Customer.

4.4.3. 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.

4.5. 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.

4.6. Assessments Pursuant to Data Protection Law

If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact (or similar) assessment or prior consultation with a regulator, at Customer's request, SAP will provide such documents as SAP makes generally available for SAP Services (for example, this DPA, the Agreement, Audit Reports and Certifications). Any additional assistance shall be mutually agreed between the Parties.

4.7. 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 fulfilling its documentation requirements, including providing the necessary information in a manner reasonably requested by the other party (such as using an electronic system), in order to enable compliance with any obligations related to maintaining records of processing.

5. DATA EXPORT AND DELETION

5.1. Export and Retrieval

If and to the extent SAP hosts Personal Data in a Cloud Service, during the Subscription Term of such Cloud Service and subject to the Agreement, 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.

5.2. Deletion

5.2.1. Before the Subscription Term of the Cloud Service expires, Customer shall perform one final data export which constitutes a final return of Personal Data from the Cloud Service.

5.2.2. At the end of the Agreement, Customer hereby instructs SAP to delete the Personal Data remaining with SAP (if any) within a reasonable time period in line with Data Protection Law (not to exceed 6 months), unless applicable law requires retention.

6. CERTIFICATIONS AND AUDITS

6.1. Customer Audit

Customer may audit SAP's compliance with the Technical and Organizational Measures relevant to Personal Data processed by SAP ("**Customer Audit**") on request only if:

(a) SAP has not provided sufficient evidence of its compliance with the Technical and Organizational Measures through providing either (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) where applicable, in respect of Cloud Services a valid ISAE3402 or ISAE3000 or other SOC1-3 attestation report either through its third party auditor or through My Trust Center ("**Audit Reports and Certifications**"); or

(b) a Personal Data Breach has occurred; or

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

(d) Data Protection Law sets out a direct audit right.

6.2. Audit Specifications

6.2.1. Prior to initiating a request for audit, Customer shall review SAP's Audit Reports and Certifications. Customer Audits shall be performed by Customer or its independent third party auditor (reasonably acceptable to SAP and excluding any third party auditor who is either a competitor of SAP or not reasonably qualified). Customer shall provide at least 60 days advance notice of any audit unless Data Protection Law or a Customer´s data protection authority requires shorter notice.

6.2.2. The start date, timeframe and scope of any Customer Audit shall be mutually agreed between the parties acting reasonably. Unless Data Protection Law or Customer´s data protection authority require more frequent audits, the frequency of a Customer Audit shall not exceed once every 12 months.

6.2.3. SAP resources to support Customer Audits shall be limited to a maximum equivalent of 3 business days in relation to Cloud Services and 1 business day in relation to other SAP Services. Customer Audits shall take place during SAP's normal business hours, not disrupt SAP's normal business operations and be subject to SAP's reasonable confidentiality requirements.

6.2.4. Customer shall provide any audit report resulting from a Customer Audit to SAP. The results of any Customer Audit shall be treated as SAP Confidential Information.

6.2.5. Customer shall bear SAP's reasonable costs of any Customer initiated 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.

6.3. Audit by other Controller

Any other Controller may assume Customer's audit rights under this Section 6 only if they apply directly to the Controller and such audit is permitted and coordinated by Customer. Customer shall use all reasonable means to combine audits of other Controllers authorized to use SAP Services by the Customer to avoid multiple audits.

7. SUBPROCESSORS

7.1. 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 the Agreement;

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

(c) SAP provides to Customer the List of Subprocessors by publishing it on My Trust Center or by making it available to Customer in writing (email permitted) upon Customer's written request.

7.2. New Subprocessors

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

(a) SAP will inform Customer in advance by email or posting on My Trust Center of any intended additions or replacements to the List of Subprocessors. Such advance notification shall be at least 30 calendar days in respect to Cloud Services and SAP Support and 5 business days in respect to Professional Services (the "**Notification Period**"). Customer shall register on My Trust Center and subscribe to its applicable and available List of Subprocessors.

(b) Customer may object to a new Subprocessor by notifying SAP in writing during the Notification Period explaining the reasonable ground(s) for its objection. SAP shall not use a new Subprocessor before the expiration of the Notification Period. If SAP does not receive any objection from Customer during the Notification Period, Customer is deemed to have accepted the new Subprocessor.

(c) If Customer objects SAP may choose: (i) not to use the Subprocessor; (ii) to take reasonable measures to remedy Customer's grounds for its objection and use the Subprocessor; or (iii) if the foregoing options are not possible, use the Subprocessor. If Customer continues to have a legitimate objection, Customer may terminate the affected SAP Service using the new Subprocessor (provided, however, termination of SAP Support for software shall also comply with the termination provision of the respective SAP Support agreement). Termination shall take effect at any time during the term of the Agreement determined by Customer in its written termination notice provided Customer accepts the use of the proposed Subprocessor until the effective termination date.

(d) If Customer objects but neither of the options under 7.2.(c) (i) or (ii) are pursued and SAP has not received notice of termination, Customer is deemed to have accepted the new Subprocessor.

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

7.3. Emergency Replacement

Where a prompt replacement is required for security or other similar urgent reasons and the reason for the change is outside of SAP's reasonable control, a Subprocessor may be replaced without advance notice by SAP. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 7.2 will apply accordingly.

8. INTERNATIONAL PROCESSING

8.1. 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.

8.2. EU Standard Contractual Clauses

Sections 8.3 to 8.4 apply where there is a transfer to a Third Country of Personal Data that is either subject to GDPR or to other Data Protection Law and where any required adequacy means under GDPR or other Data Protection Law can be met by entering into the EU Standard Contractual Clauses, as amended in accordance with Data Protection Law.

8.3. Applicability of EU Standard Contractual Clauses Where SAP is Not Located in a Third Country

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 EU Standard Contractual Clauses with each Third Country Subprocessor as the data importer. Module 3 (Processor to Processor) of the EU Standard Contractual Clauses shall apply to such transfers.

8.4. Applicability of EU Standard Contractual Clauses where SAP is Located in a Third Country

8.4.1. Where SAP is located in a Third Country, or a country that otherwise requires use of the EU Standard Contractual Clauses, SAP and Customer enter into the EU Standard Contractual Clauses with Customer as the data exporter and SAP as the data importer as follows:

(a) Module 2 (Controller to Processor) shall apply where Customer is a Controller; and

(b) 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 EU Standard Contractual Clauses, SAP acknowledges that Customer acts as Processor under the instructions of its Controller(s).

Other Controllers or Processors whose use of SAP Services is authorized by Customer under the Agreement may also enter into the EU Standard Contractual Clauses with SAP in the same manner as Customer in accordance with Section 8.4.1 above. In such case, Customer enters into the EU Standard Contractual Clauses on behalf of other Controllers or Processors.

8.4.2. Where Customer is located in a Third Country and is acting as a Processor under Module 2 or Module 3 of the EU Standard Contractual Clauses and SAP is acting as Customer's sub-processor, the respective data exporter shall have the following third party beneficiary right:

In the event that 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 SAP 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.

8.4.3. On request from a Data Subject, Customer may make a copy of Module 2 or 3 of the EU Standard Contractual Clauses entered into between Customer and SAP (including the relevant Schedules attached hereto), available to Data Subjects.

Schedule 1 Description of the Processing

This Schedule 1 applies to the Processing of Personal Data under the Agreement and for the purposes of the EU Standard Contractual Clauses and Data Protection Law.

Where Customer and SAP enter into the EU Standard Contractual Clauses, Schedule 1 is incorporated as Annex I of the EU Standard Contractual Clauses.

1. OPTIONAL CLAUSES OF THE EU STANDARD CONTRACTUAL CLAUSES

1.1. The governing law of the EU Standard Contractual Clauses shall be the law of Germany and German courts shall have jurisdiction over any disputes resulting from the EU Standard Contractual Clauses.

1.2. The optional Clause 7 and the option in Clause 11a of the EU Standard Contractual Clauses shall not apply.

1.3. Option 2, General Written Authorization of Clause 9 of the EU Standard Contractual Clauses shall apply in accordance with the notification periods set out in Section 7 of this DPA.

2. A. LIST OF PARTIES

2.1. Under the EU Standard Contractual Clauses (Section 8.4 of the DPA)

2.1.1. Module 2: Transfer Controller to Processor

Where Customer is the Controller and SAP is the Processor, then Customer is the data exporter and SAP is the data importer.

2.1.2. Module 3: Transfer Processor to Processor

Where Customer is a Processor and SAP is a Processor, then Customer is the data exporter and SAP is the data importer.

3. B. DESCRIPTION OF TRANSFER AND PROCESSING

3.1. Categories of Data Subjects Whose Personal Data is transferred or Processed:

Unless provided otherwise by the data exporter, Personal Data relates to the following categories of Data Subjects: employees, contractors, Business Partners or other individuals having Personal Data stored, transmitted to, made available to, accessed or otherwise processed by the data importer.

3.2. Categories of Personal Data that are Transferred or Processed:

Customer determines the categories of data and/or data fields which could be transferred or processed per SAP Service as stated in the Agreement. For Cloud Services, Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data transferred or entered into the SAP Service by Authorized Users and may include financial data such as bank account data, credit or debit card data.

3.3. Special Data Categories (if agreed)

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

3.3.2. 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):

(a) training of personnel;

(b) encryption of data in transit and at rest; and

(c) system access logging and general data access logging.

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

3.4. Purposes of Data Transfer and Further Processing; Nature of Processing

3.4.1. For Cloud Services

Personal Data is subject to the following basic Processing activities:

(a) use of Personal Data to set up, operate, monitor, provide and support the Cloud Service (including operational and technical Support);

(b) continuous improvement of Cloud Service features and functionalities provided as part of the Cloud Service including automation, transaction processing and machine learning;

(c) provision of Professional Services or Consulting Services;

(d) communication to Authorized Users;

(e) storage of Personal Data in dedicated data centers (multi-tenant architecture);

(f) release, development and upload of any fixes or upgrades to the Cloud Service;

(g) back up and restoration of Personal Data stored in the Cloud Service;

(h) computer processing of Personal Data, including data transmission, data retrieval, data access;

(i) network access to allow Personal Data transfer;

(j) monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database;

(k) security monitoring, network-based intrusion detection support, penetration testing; and

(l) execution of instructions from Customer in accordance with the Agreement.

The purpose of the transfer and processing is to provide and support the Cloud Service. SAP and its Subprocessors may support the Cloud Service data centers remotely. SAP and its Subprocessors provide support when a Customer submits a support ticket as further set out in the Agreement.

3.4.2. For SAP Support and Professional Services:

Personal Data is subject to the basic processing activities as set out in the Agreement which may include:

(a) accessing systems containing Personal Data in order to provide SAP Support and Professional Services;

(b) use of Personal Data to provide and support the SAP Service;

(c) continuous improvement of service features and functionalities provided as part of the SAP Service including automation, transaction processing and machine learning;

(d) storage of Personal Data;

(e) computer processing of Personal Data for data transmission; and

(f) execution of instructions from Customer in accordance with the Agreement.

3.4.3. For SAP Support:

SAP or its Subprocessors provide support when a Customer submits a support ticket because the software is not available or not working as expected. SAP or its Subprocessors answer phone calls, perform basic troubleshooting, and handle support tickets in a tracking system.

3.4.4. For Professional Services:

SAP or its Subprocessors provide Professional Services subject to the Agreement for Professional Services and the applicable scope document.

3.5. The purpose of the transfer is to provide and support the relevant SAP Service. SAP and its Subprocessors may provide or support the SAP Service remotely.

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

Personal Data will be transferred on an ongoing basis for the duration of the Agreement.

3.7. The period for which Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

Personal Data will be retained by SAP as set out in Section 5 of the DPA.

3.8. For transfers to (sub-) processors, also specify subject matter, nature and duration of processing:

SAP will transfer Personal Data to Subprocessors as stated in the applicable List of Subprocessors for the duration of the Agreement.

4. C. COMPETENT SUPERVISORY AUTHORITY

4.1. In respect of the EU Standard Contractual Clauses:

Where Customer is the data exporter under Module 2 or Module 3, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the EU Standard Contractual Clauses.

Schedule 2 Technical and Organizational Measures

The Technical and Organizational Measures (as defined in Section 1.166) are hereby incorporated by reference.

These Technical and Organizational Measures also describe the applicable technical and organizational measures for the purposes of the EU Standard Contractual Clauses and Data Protection Law. Where Customer and SAP enter into the EU Standard Contractual Clauses, Schedule 2 is incorporated as Annex II of the EU Standard Contractual Clauses.

To the extent that provisioning of SAP Service(s) involves an international transfer to which the EU Standard Contractual Clauses apply, the Technical and Organizational Measures describe the measures and safeguards that consider the nature of Personal Data and the risks involved. If local laws affect compliance with EU Standard Contractual Clauses, additional safeguards may be triggered during the transmission and processing of Personal Data in the country of destination (if applicable: encryption of data in transit, encryption of data at rest, anonymization, pseudonymization).

Schedule 4

Security Measures for Cloud Services ("Security Measures")

These Security Measures are the Technical and Organizational Measures referenced in the DPA and define the current technical and organizational measures maintained by SAP to protect Customer Data. SAP may change the Security Measures at any time without notice, provided SAP maintains a comparable or better security level. Individual measures may be replaced by new measures that serve the same purpose without diminishing the overall security level protecting Customer Data.

1. INFORMATION SECURITY GOVERNANCE

1.1. Security Framework

SAP maintains a formal security framework with written policies and standards designed to protect the confidentiality, integrity, and availability of Customer Data ("**SAP Security Framework**"). The SAP Security Framework:

(i) is approved by SAP management;

(ii) supports the measures described in the Security Measures; and

(iii) is reviewed at least annually by SAP stakeholders to assess opportunities for improvement, changes in technology, and risks.

As part of this stakeholder review, SAP considers guidance from independent third-party sources such as the National Institute of Standards and Technology (NIST), British Standards Institute (BSI), and the International Organization for Standardization (ISO).

1.2. Executive Oversight

SAP maintains a Chief Security Officer (or equivalent executive) responsible for overseeing the SAP Security Framework and communicating essential security topics to the SAP Executive Board.

2. SECURITY CERTIFICATIONS & ATTESTATIONS

2.1. Internal Assessment

SAP regularly assesses the effectiveness of security controls within the SAP Security Framework.

2.2. Independent Third-Party Review

SAP conducts certain external audits with third-party auditors to provide independent security assurances.

2.3. Self-Service Reviews

SAP obtains certain third-party certifications and attestations. Customer may conduct self-service reviews of obtained security certifications and attestations for a subscribed Cloud Service as SAP is permitted to make available to customers of the Cloud Service (e.g., ISO 27001, SOC 2, or other comparable reports). Customers may request available certifications and reports on the SAP Trust Center.

3. ORGANIZATIONAL SECURITY MEASURES

3.1. Limited Use of Customer Data

SAP processes Customer Data only in accordance with the Agreement including the applicable confidentiality and nondisclosure obligations.

3.2. Security Risk Management

SAP maintains a risk management program designed to identify, analyze, and manage threats to the Cloud Service.

3.3. Human Resource Security

3.3.1. Before granting access to Customer Data, SAP:

(i) performs a pre-employment screening on employees unless restricted by law;

(ii) enters into a confidentiality agreement with employees; and

(iii) mandates employee training on information security.

3.3.2. SAP maintains a Global Code of Ethics and Business Conduct ("**SAP Code of Conduct**") outlining SAP's values and standards for ethical business. SAP mandates employees to adhere to the SAP Code of Conduct, and SAP internally investigates suspected breaches of the SAP Code of Conduct.

3.3.3. Employees complete role-based security and privacy training, acknowledge communication of written security policies, and receive regular awareness education.

3.4. Asset Management

As part of SAP's internal asset management process, SAP is responsible for:

(i) inventorying assets;

(ii) assigning ownership;

(iii) categorizing assets into defined written classes;

(iv) tracking and monitoring assets; and

(v) defining acceptable use of assets.

3.5. Third-Party Risk Management

SAP maintains a third-party risk management program that manages supplier risks to the Cloud Service ("**TPRM Program**"). At minimum, the TPRM Program includes:

(i) established third-party engagement policies;

(ii) risk assessments; and

(iii) controls and processes to monitor contract compliance between SAP and its third-party suppliers.

3.6. Secure Cloud Development

SAP maintains a secure development and operations lifecycle framework designed to mitigate software development risks to the Cloud Service ("**SDOL Framework**"). At minimum, the SDOL Framework is designed to:

(i) define criteria for software security assessments and releases;

(ii) protect code from unauthorized access and tampering;

(iii) verify and test software release integrity; and

(iv) identify and manage known vulnerabilities.

3.7. Change Management

As part of the broader SAP Security Framework, SAP maintains formal change management processes ("**SAP Change Management**"). At minimum, SAP Change Management requires that material changes to the Cloud Service are planned, tested, and approved.

4. PHYSICAL SECURITY MEASURES

4.1. Data Center Measures

Data centers are protected using multiple measures designed to prevent unauthorized individuals from gaining physical access to data centers hosting Customer Data. These physical access measures include key/access systems, security zones, access credentials, door locks, guards, cameras, motion sensors, alarm systems, and other applicable measures designed to protect equipment and facilities from compromise. To protect proper functionality, physical security equipment undergoes regular maintenance and security checks, and is supported by uninterrupted power supplies (e.g., UPS, batteries, generators, etc.).

4.2. Personnel Access

Access rights are granted to authorized persons on an individual basis in accordance with written policies (see access control details below). Only authorized persons with appropriate credentials have access to systems and infrastructure within data centers hosting Customer Data. Guests and visitors must register and log their names and times at reception upon entry.

4.3. Physical Media Disposal

Physical media is disposed in accordance with physical decommissioning policies. Before disposing physical media, commercially reasonable erasure methods render Customer Data on physical media unrecoverable.

5. TECHNICAL SECURITY MEASURES

5.1. Security Logging and Monitoring

Cloud Service monitoring is designed to check the ongoing confidentiality, integrity, and availability of the Cloud Service, which includes logging information system and infrastructure events. Logged activities from network devices and systems are fed into SAP's Security Information and Event Management (SIEM) system(s), or similar central monitoring system(s), which generate appropriate alerts.

5.2. Intrusion Monitoring

SAP uses intrusion detection mechanisms to monitor the Cloud Service for unauthorized intrusions.

5.3. System Hardening

SAP maintains system hardening policies and processes to promote the security of the Cloud Service.

5.4. Data Integrity

SAP deploys a multi-layered defense strategy that protects against unauthorized modifications of Customer Data. Customer Data may only be read, copied, modified, or removed by SAP in accordance with the Agreement.

5.5. Secure Data Deletion

SAP securely deletes Customer Data in accordance with the Agreement.

5.6. Data Segregation

SAP employs various methods designed to segregate Customer Data from data of other SAP customers including:

(i) physical designs;

(ii) logical designs; and

(iii) server, operating system, and database restrictions.

5.7. Access Control

5.7.1. Access Management

Access controls provide identity management and grant appropriate access rights ("**Access Management Controls**"). Access Management Controls are designed to follow the principles of "least privilege," "need-to-know," and "segregation of duties."

5.7.2. Personnel Access

SAP personnel are issued a unique identifier to access SAP's systems. SAP maintains written procedures to administer access authorization changes and access rights are revoked when personnel are no longer authorized to access applicable systems (e.g., termination of employment).

5.7.3. Administrative Rights

Administrative rights are only assigned to privileged and technical SAP users on a "least privilege" and "need-to-know" basis.

5.7.4. Password Management

SAP maintains a written password management policy that defines minimum requirements such as length, complexity, expiration, and lockout requirements.

5.8. Secure Data Transmission

SAP secures the exchange or transmission of Customer Data between SAP systems that constitute the Cloud Service. Measures for securing the exchange of information may include email encryption, provisioning of secure network protocols and interfaces, or features and functionality that support "data in transit" encryption (e.g., communication encryption protocols, server-to-server authentication, certificate authentication). 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). SAP recommends that Customer enables encryption of Customer Data in transit between Customer's network and the Cloud Service to protect against unintended disclosure or modification of Customer Data where applicable.

5.9. Secure Data Storage

Customer Data is encrypted at rest while stored in the Cloud Service.

5.10. Malware Management

SAP uses up-to-date anti-malware software designed to protect Customer Data from malware that may negatively impact the confidentiality, integrity, or availability of Customer Data.

5.11. Endpoint Devices

SAP maintains security mechanisms on its devices that access Customer Data. Mechanisms may include firewalls, anti-malware software, disk encryption, restrictions to limit disablement of security mechanisms, and default systems for timeout locks. SAP maintains a list of prohibited software that may not be installed on SAP devices.

5.12. Vulnerability and Patch Management

SAP maintains processes to monitor, detect, and respond to security vulnerabilities. At minimum, these processes require:

(i) periodically reviewing third-party vulnerability alert services and official public disclosures posted on software vendor websites relevant to the Cloud Service;

(ii) establishing internal vulnerability evaluation criteria;

(iii) periodically conducting vulnerability scans; and

(iv) patching the Cloud Service in accordance with operational procedures.

5.13. Penetration Testing

SAP will conduct penetration testing and maintain internal policies that govern how the Cloud Service is proactively tested.

5.14. Additional Details

Customer may review additional technical details in each Cloud Service's respective Documentation.

6. RESILIENCY

6.1. Backups

SAP periodically backs up Customer Data and maintains alternative data centers to enable secondary storage of backup data. Backups are automated and the Cloud Service backup process includes hardware-independent restore and recovery capabilities. SAP's backup and recovery process is tested regularly.

6.2. Continuity and Recovery

SAP maintains disaster recovery or data resiliency procedures reasonably designed to safeguard the availability of the Cloud Service and Customer Data ("**SAP Resiliency Procedures**"). At minimum, SAP Resiliency Procedures include:

(i) Customer Data backups (as described above);

(ii) secondary storage locations;

(iii) personnel with sufficient training to implement and support the SAP Resiliency Procedures;

(iv) testing or validating SAP Resiliency Procedures at least once per calendar year;

(v) maintaining written policies or standards that govern SAP Resiliency Procedures; and

(vi) crisis and process continuity plan(s) to protect operations during a major disruption event.

7. SECURITY INCIDENT MANAGEMENT

7.1. Security Incident Management Program

SAP maintains a security incident management program designed to detect, investigate, and respond to declared security incidents that impact the Cloud Service ("**SAP Incident Management Program**"). At minimum, the SAP Incident Management Program is:

(i) approved by management;

(ii) supported by teams with documented roles and responsibilities; and

(iii) annually reviewed and tested.

7.2. Security Incident Assessment Process

As part of the SAP Incident Management Program, SAP maintains written policies and standards that govern how SAP assesses and analyzes potential security incidents that may impact the Cloud Service ("**Security Incident Assessment Process**"). At minimum, the Security Incident Assessment Process is designed to do the following:

(i) assess, classify, and prioritize security incidents in accordance with SAP's written incident response plan;

(ii) if appropriate, perform a security root cause analysis when Customer Data is impacted; and

(iii) establish a process to attempt to reduce the likelihood of similar security incidents from impacting the Cloud Service in the future.

7.3. Customer Notification

SAP will electronically notify Customer's registered contact(s) without undue delay after confirming a security breach has resulted in the unauthorized destruction, loss, alteration, or third-party access to Customer Data ("**Customer Data Breach Notification**"). As part of the Customer Data Breach Notification, SAP will provide relevant and available information to Customer (e.g., material details, planned mitigation steps, and/or recommended Customer actions). SAP's delivery of a Customer Data Breach Notification will not be construed as an acknowledgement or admission of any fault or liability.

8. REPORTING & UPDATES

8.1. Customer Event Reporting

Security events can be reported through SAP's customer support portal, by e-mail (cybersecurity@sap.com), via www.sap.com, or by phone via SAP's worldwide Customer Interaction Center.

8.2. Security Contacts

Customer must register one or more security contacts within the support portal made available to Customer.

8.3. Updates

SAP will publish updated versions of the Security Measures on My Trust Center and Customer subscribe to receive automated notification (or other link provided by SAP from time-to-time).

8.4. Shared Responsibility

Customer acknowledges that the Cloud Service makes certain security features available that Customer is responsible for enabling or otherwise configuring.

Schedule 5

SAP Product Development Schedule

This Product Development Schedule details how SAP, SAP SE, or SAP Affiliates ("**SAP Group**") uses Customer Data for general product research and development, including creating new products, services, or components not specific to a given service or customer (together, "**Product Development**").

1. PRODUCT DEVELOPMENT PROCESSING

Notwithstanding anything in the Agreement, the SAP Group may also process Customer Data in accordance with this Product Development Schedule for Product Development purposes globally, provided the output of such processing does not identify Customer, Authorized Users, natural persons, or otherwise reveal Customer Confidential Information ("**Product Development Processing**"). The following additional rules shall apply to Product Development Processing:

(a) Personal Data used for Product Development Processing must be either (i) anonymized during or directly after extraction from Customer's instance of the Cloud Service before being further used for Product Development, or (ii) extracted for immediate Product Development Processing using automated extraction and processing technologies (e.g., algorithms or software), and then automatically deleted thereafter. Except as set out above or otherwise set out in the Agreement, Personal Data is only used to provide and support the Cloud Service and Consulting Service.

(b) During Product Development Processing, the SAP Group will not (a) use Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or (b) isolate the content of Customer Data in a manner that puts the SAP Group in a position to identify individual data subjects during or after Product Development Processing.

(c) Product Development Processing is subject to the same confidentiality and non-disclosure protections applicable to Customer Data.

(d) Product Development Processing will be performed using appropriate technical and organizational measures to provide a level of security appropriate to the risk of Product Development Processing.

(e) Any result, output or derivative of Product Development or Product Development Processing shall be treated as Cloud Materials. Customer shall retain all ownership rights in Customer Data.

(f) Notwithstanding anything in the Agreement, only the data processing, non-disclosure, and security terms identified in this Product Development Schedule shall apply to Product Development Processing.

2. PERMISSION MANAGEMENT

Where SAP makes such functionality available to Customer (e.g., customer dashboard), Customer may remove Product Development Processing permissions under this Product Development Schedule.

Schedule 6

SAP AI TERMS

These SAP AI Terms ("**Terms**") apply to artificial intelligence features and technologies provided with SAP Cloud Services ("**AI Technology**"). "**Output**" means any content generated by AI Technology as output, based on the data provided to AI Technology, including Customer Data, and data used to train AI Technology.

1. ACCEPTABLE USE

1.1. Customer will use AI Technology responsibly, safely, in a legally compliant manner, and in accordance with the Documentation, and will not use AI Technology to:

(a) Promote or facilitate illegal activities or unlawful actions;

(b) Facilitate fraudulent actions;

(c) Attempt unauthorized access to a system, property, or information;

(d) Generate content that contains or promotes violence, hate speech, or harassment, or insults or demeans a person;

(e) Generate sexually explicit content;

(f) Distribute malware or spam;

(g) Contravene regulatory safety policies;

(h) Track people without consent;

(i) Falsely impersonate an individual; or

(j) Mine cryptocurrency.

1.2. SAP may limit or suspend access to Output or AI Technology in the event these Terms are violated or for non-compliance with Documentation.

1.3. Customer will not circumvent or bypass protective measures made available by SAP or a third-party, including, but not limited to, those intended to help prevent copyright infringement, data breaches, or security incidents.

1.4. Customer will not (i) use AI Technology or Output to develop, train, or improve other AI services or AI models, unless explicitly permitted by SAP, or (ii) use web scraping, web harvesting, or web data extraction methods to extract data from AI Technology or Output.

2. OUTPUT

2.1. Notwithstanding any recommendation contained within Output, reliance on Output is in Customer's discretion. Customer will assess Output (including by code scanning, security scanning, human review, and human oversight and correction) before using or relying on the Output for any purpose. Customer will also utilize any review tools and filtering options that SAP makes available.

2.2. Customer acknowledges that AI Technology consists of emerging technologies and, given the nature of such technologies, their use may result in incorrect, biased, unfair, or inaccurate Output and/or Output that may be nonsensical or untruthful in relation to certain sources.

2.3. Customer acknowledges and agrees that (i) Output may not qualify for intellectual property protection; (ii) similar or the same Output may be produced by AI Technology to similar requests from different customers, and (iii) Customer's rights to Output may not be enforceable against other users of AI Technology. Customer's ownership in Output is subject to SAP's and/or its licensor's ownership rights in the Cloud Service, SAP Materials, and data used to train AI Technology ("**Pre-Existing Materials**"). Customer is granted a right to use, and only will use, Pre-Existing Materials in Output to the same extent as Customer is permitted to use the Cloud Service.

2.4. SAP's indemnification obligations, to the extent provided in the Agreement, shall apply to the AI Technology, but not to Output.

3. ADDITIONAL TERMS

3.1. Customer acknowledges that the legal framework applicable to and the interpretation of competent courts and authorities regarding the use of AI technologies is evolving. If a change in law or the interpretation of a competent court or authority results in (i) SAP's inability to offer an AI Technology or (ii) Customer's inability to use an AI Technology in a legally compliant manner, SAP may reduce the scope of use (e.g., if the use of an AI Technology becomes prohibited, SAP may cease offering such AI Technology in a given country) or remove such AI Technology altogether. The same applies where SAP can no longer provide an AI Technology provided by a third-party, because such third-party discontinues availability of such AI Technology or changes its service terms or documentation in contradiction to the Agreement or another way that prevents SAP from further offering such AI Technology.

3.2. AI Technology may include AI models, technologies or features licensed from third-parties that require SAP to pass through additional terms. Customer will comply with such pass-through terms as made available by SAP at https://www.sap.com/about/trust-center/agreements.html, within the Documentation, or otherwise. When SAP introduces new AI Technology, SAP may provide additional terms or make updates to the terms, that apply to Customer's use of such AI Technology.

3.3. SAP does not commit to the use of specific AI models in a Cloud Service even if Customer may be able to choose between different AI models when using the Cloud Service. SAP reserves the right to add, remove, or exchange AI models, in its sole discretion, at any time.

3.4. SAP may update these Terms in connection with the evolving landscape by publishing the updated Terms on the SAP agreements website. Customer may subscribe to receive automated notification of any updates via My Trust Center, accessible at https://support.sap.com/en/my-support/trust-center.html (or other link provided by SAP). The updated Terms will apply to AI Technology effective 1 month after SAP's publication to the extent permitted under applicable law. If Customer continues using the AI Technology after the effective date of the update, Customer will be bound by such updated Terms thereafter. If a change significantly diminishes Customer's rights or significantly increases Customers obligations under these Terms, but is not required by applicable law or an interpretation of law by a competent court or authority, Customer may terminate its subscription to the impacted Cloud Service by providing written notice of termination to SAP within 1 month of SAP's publication of the update.

Schedule 7

PROFESSIONAL SERVICES SCHEDULE

This Schedule is a supplement to the General Terms and Conditions for Cloud Services ("**GTC**") which applies solely to Professional Services and not to any other SAP product or service.

Capitalized terms in this Schedule but not defined have the meaning defined in the GTC.

1. DEFINITIONS

1.1. **"Consultants"** means employees and third-party contractors which SAP utilizes to provide Professional Services to Customer.

1.2. **"Deliverables"** means those specific Work Products which are explicitly identified as a "Deliverable" in the applicable Scope Document.

1.3. **"Scope Document"** means the document published at https://www.sap.com/about/trust-center/agreements/services/scope-documents.html?sort=latest_desc and which describes the Professional Services to be provided.

1.4. **"Work Product"** means any work product or tangible results produced by or with SAP, including works created for or in cooperation with Customer.

2. PROVISION OF PROFESSIONAL SERVICES

2.1. Performance

2.1.1. In addition to the Cloud Services described in the Order Form, SAP shall provide distinct Professional Services as listed in the Order Form. SAP will provide the Professional Services in accordance with the Scope Document, this Schedule and the GTC.

2.1.2. If any Professional Service, in whole or in part, cannot be provided by SAP due to a Customer issue and Customer fails to provide SAP with reasonable advance notice, the time spent by Consultants on such Professional Service will be charged to Customer.

2.2. Service Location

Unless otherwise identified for a particular Service, the Customer office location identified in an Order Form will be considered the location of Customer's receipt of Services provided hereunder. Customer understands that the calculation of Taxes may be affected by this receipt of Service Location.

2.3. Subcontracting

Section Subcontracting of the GTC applies to the provision of Professional Services.

2.4. Legal and regulatory matters

SAP will not provide any advisory services regarding any Customer's compliance with tax, legal, or other regulatory matters. SAP Services will be limited to technical assistance based on requirements as specified by Customer. Customer is solely responsible for determining and validating its compliance with tax, legal and other regulatory matters.

2.5. Time not of essence

All dates with respect to performance of the Professional Services are estimated and time shall not be deemed of the essence.

3. CUSTOMER RESPONSIBILITIES

3.1. Access, System Security and Data Safeguards

3.1.1. Customer will make the necessary arrangements to allow SAP to perform the Professional Services, including the availability of consistent, stable and fast remote connectivity and the necessary authorizations for remote access to Customer's systems.

3.1.2. When SAP is given access to Customer's systems and data, SAP shall comply with Customer's reasonable administrative, technical, and physical safeguards to protect such data and guard against unauthorized access. In connection with such access, Customer shall be responsible for providing Consultants with user authorizations and passwords to access its systems and revoking such authorizations and terminating such access, as Customer deems appropriate from time to time. Customer shall not grant SAP access to Customer systems or personal information (of Customer or any third party) unless such access is essential for the performance of the Professional Services. Customer shall not store any personal data in non-production environments. No breach of this provision shall be deemed to have occurred in the event of SAP's non-conformance with the aforementioned safeguard but where no personal information has been compromised.

3.2. Customer Cooperation

3.2.1. Customer shall provide and make available all Customer personnel that SAP reasonably requires in connection with performance of the Professional Services and as may be further addressed in a Scope Document.

3.2.2. Customer shall appoint a contact person with the authority to make decisions and to supply SAP with any necessary or relevant information expeditiously.

3.3. Use Rights Prerequisites

Customer shall ensure to have all necessary use rights for the Cloud Service as well as any relevant third party license or use rights required to perform the Professional Services.

4. FEES AND TAXES

4.1. The fees for the Professional Services as specified in the Scope Document are at the fixed price as defined in the Order Form.

4.2. Customer must pay the Professional Services fees in accordance with the Section "Fees and Taxes" of the GTC.

5. TERM AND TERMINATION

5.1. For subscription-based Professional Services, the Subscription Term (or remainder thereof) set forth in the Order Form applies to the delivery of the Professional Services. Subscription-based Professional Services shall be co-terminus with the respective Cloud Services. For non subscription-based Professional Services, the delivery schedule and term are set forth in the Scope Document.

5.2. Termination of the Professional Services

Section 6.2 of the GTC (Termination for material breach) applies.

5.3. Effect of termination

5.3.1. Upon the effective date of termination of the Professional Services, Customer shall be liable for payment of all costs, fees and expenses up to the effective date of termination for:

(a) any completed, partially completed or scheduled Services from any phase or milestone;

(b) any reasonable committed costs or expenses

5.3.2. Upon the effective date of termination of the Professional Services, Section 11.4 of the GTC regarding destruction and return of Confidential Information applies.

5.4. Survival

Sections 1, 4, 5.3, 5.4, 8 and 9 of this Schedule survive the expiry or termination of the Agreement.

6. USAGE RIGHTS AND RESTRICTIONS

6.1. Section 2.1 of the GTC (Grant of Rights) applies to all Deliverables and Work Products provided to Customer by SAP.

6.2. Customer may allow its third party service providers to access the Deliverables, Work Product and Professional Services of SAP solely to the extent such third party service providers require such access in the course of providing services to Customer. Customer is responsible for breaches of the Agreement caused by its third party service providers.

7. PROFESSIONAL SERVICES WARRANTY

7.1. Good industry practices

7.1.1. SAP warrants that:

(a) its Professional Services will be performed in a professional workman-like manner by Consultants with the skills reasonably required for the Professional Services; and

(b) for 90 days following provision of the Professional Service or Deliverable, the Deliverables will materially conform with the applicable specifications for that Professional Service or Deliverable. For clarity, the warranty period for Deliverables (if any) resulting from any subscription based Professional Services will in no event exceed the termination date of the subscription based Professional Services.

7.1.2. SAP does not warrant error-free or uninterrupted operation of any Professional Service or Deliverable or that SAP will correct all non-conformities.

7.2. Notification

Customer shall notify SAP within 90 days of provision of the Professional Service or Deliverable in writing of the alleged warranty breach and provide SAP with a precise description of the problem and all relevant information reasonably necessary for SAP in order to rectify such warranty breach.

7.3. Remedy

Provided Customer has notified SAP in accordance with Section 7.2 of a warranty breach and SAP validates the existence of such warranty breach, SAP will, at its option:

(a) re-perform the applicable Professional Service or Deliverable; or

(b) refund the fee paid for the specific non-conforming Professional Service or Deliverable.

This is Customer's sole and exclusive remedy for a warranty breach.

7.4. Exclusions

This warranty shall not apply:

(a) if the Deliverables are not used in accordance with any applicable documentation provided; or

(b) if the alleged warranty breach is caused by a modification to the Deliverable, Customer or third party software.

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 Deliverables infringes or misappropriates a patent claim, copyright or trade secret right. SAP will indemnify Customer against all damages finally awarded against Customer (or the amount of any settlement SAP enters into) with respect to these claims.

8.1.2. SAP's obligation under Section 8.1.1 will not apply if the alleged claim results from:

(a) use of the Deliverables in conjunction with any product or services not provided by SAP;

(b) use of the Deliverable 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;

(d) modification of the Deliverable by Customer or by a third party on behalf of Customer;

(e) anything that Customer provides to SAP including configurations, instructions or specifications in relation to Services; or

(f) any use of the Professional Services not permitted under the Agreement.

8.2. If a third party makes a claim under Section 8.1 or in SAP's reasonable opinion is likely to make such claim, SAP may, at its sole option and expense:

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

(b) replace or modify the Deliverable to be non-infringing without material decrease in functionality.

8.3. If these options are not reasonably available, SAP or Customer may terminate the Professional Services relating to the affected Deliverable upon written notice to the other.

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

8.5. Claims Brought Against SAP

Customer will defend SAP against claims brought against SAP, SAP SE, its Affiliates and subcontractors by any third party to an allegation that Customer Data, Customer's use of the Professional Services or anything Customer has provided to SAP including access to third party software or proprietary information violates, infringes or misappropriates the rights of a third party. 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 those claims.

8.6. Section 8.3 (Third Party Claim Procedure) and section 8.4 (Exclusive remedy) of the GTC apply to this section 8.

9. LIMITATION OF LIABILITY

9.1. No Cap on Liability

Section 9.1 of the GTC applies to the Professional Services.

9.2. Liability Cap

Except as set forth in Section 9.1 above, the maximum aggregate liability of either party (or its respective Affiliates or SAP's subcontractors) to the other or any other person or entity for all events (or series of connected events) shall not exceed the fees paid for the applicable Professional Services under the relevant Order Form or in the case of subscription based Professional Services or Professional Services with monthly reoccurring fees, the fees paid in the 12 month period preceding the date of the incident giving rise to the liability.

9.3. Exclusions of Damages

Section 9.3 of the GTC applies to the Professional Services.

Schedule 8

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, 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 relating to the Cloud Services located at https://help.sap.com or which SAP makes available to Customer as part of the Cloud Service, including technical and functional specifications as updated from time to time in accordance with 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 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 or information (including statistical reports and usage measurements of the Cloud Service) provided, developed, derived, 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 may allow individuals employed by its outsourced service providers to be Authorized Users solely to the extent such providers are required to access the Cloud Service in the course of providing outsourced services to Customer. 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:

(a) if continued use may result in material harm to the Cloud Service or its users; or

(b) to comply with laws and regulations applicable to SAP, its Affiliates' or subcontractors.

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 for the duration of the applicable Subscription Term. SAP determines the location of the data centers unless otherwise agreed in the Order Form.

3.2. Support

SAP provides support for the Cloud Service as referenced in the Order Form. The scope of SAP support offered by SAP may be changed annually by SAP at any time without notice so long as it maintains a comparable or better level of support. Individual measures may be replaced by new measures that serve the same purpose without diminishing the support level. SAP will publish updated versions of the Support Schedule for Cloud Services on SAP agreements website.

3.3. Security

SAP will protect Customer Data in accordance with the Security Measures. “Security Measures” means the technical and organizational measures for the relevant Cloud Service published on https://www.sap.com/about/trust-center/agreements/SecurityMeasures.

3.4. Modifications

3.4.1. Scope

SAP may modify the Cloud Service (including support services, Maintenance Windows and Major Upgrade Windows), provided that SAP shall not materially degrade the core functionality of the Cloud Service during the Subscription Term.

3.4.2. Modification Notices

SAP shall provide Customer with reasonable advance notice of modifications to the functionality of the Cloud Service in accordance with Section 13.5, except for any change to a Maintenance Window or Major Upgrade Window which shall be in accordance with the Service Level Agreement.

3.4.3. Customer Termination

If the modification materially degrades the Cloud Service and SAP does not provide equivalent functionality, Customer may terminate its subscription to the affected Cloud Service by providing written notice to SAP within 1 month of SAP’s notice. If SAP does not receive timely notice, Customer is deemed have accepted the modification.

4. CUSTOMER AND PERSONAL DATA

4.1. Customer Ownership

As between the parties, Customer owns all right and interest in and to 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 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. SAP will delete Customer Data remaining on production servers hosting the Cloud Service within 3 months from termination or expiration of Agreement unless retention is permitted under the Agreement or required under applicable law. Retained data is subject to the confidentiality provisions of the Agreement.

4.5.4. Upon Customer's reasonable written request received by SAP at least 1 month prior to termination of the Agreement, SAP will provide limited access to the Cloud Service for no more than 1 month past termination of the Agreement strictly as needed for Customer to export Customer Data ("**Retrieval Period**"). The Retrieval Period is subject to the following:

(a) Customer agrees that even if access is not technically limited to exporting Customer Data it shall not utilize the Cloud Service for any other purpose during the Retrieval Period;

(b) If Customer uses the Cloud Service for anything other than exporting Customer Data during the Retrieval Period, Customer agrees to pay SAP's then-current prorated price list rates for the entire Retrieval Period; and

(c) Customer's access during the Retrieval Period shall continue to be governed by its obligations under the Agreement. At the end of the Retrieval Period, the Agreement will terminate, and SAP will delete Customer Data as otherwise required under the Agreement.

4.5.5. 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, Invoices and Payment

Customer shall pay all fees due to SAP within 30 days of date of invoice. SAP will provide invoices to the email address provided by Customer. Invoices are deemed delivered when sent to the email address provided by Customer. Customer may view invoices on SAP For Me customer portal and is responsible for providing and maintaining complete and accurate billing and contact information. Failure to provide accurate information is not grounds for non-payment. Any fees not paid when due shall accrue interest at the maximum legal rate.

If Customer provides payment information permitting SAP to process payments, Customer authorizes SAP to charge for all Cloud Services and other services listed in the Order Form for both the initial subscription term and any renewal subscription terms.

Purchase orders are for administrative convenience only and not a condition of payment. SAP may issue an invoice and collect payment without a corresponding purchase order. All Customer payments must

reference the applicable invoice number. If Customer does not have an invoice reference on its payment, SAP may apply payment to the oldest invoice.

Payment is not dependent upon completion of any implementation or other services. If applicable, fees for non-recurring services will be invoiced by SAP on a one-time basis and paid by Customer upon commencement of the first Product Start Date, indicated on the Order Form. Customer shall reimburse SAP for all appropriately documented travel and related expenses pre-approved by Customer and incurred by SAP in performing support for Cloud Services.

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 and other services until payment is made. SAP shall provide Customer with prior written notice of suspension.

Customer may not withhold, reduce or set-off fees owed. Customer may not reduce the volume of Usage Metrics during the Subscription Term. All Order Forms are non-cancellable. All fees are non-refundable except per Sections 6.3 or 7.3.3.

5.2. Disputed Invoices

If Customer has reasonable grounds to dispute an invoice in whole or in part, Customer must notify SAP within 1 month of the date of the invoice by submitting a dispute with reference to that invoice and a description of the reasons for the dispute.

Customer shall promptly pay the undisputed portion of the invoice. SAP shall not exercise its right to charge late payment interest charges or suspend use of the Cloud Service if Customer is disputing an invoice, or portion of an invoice, reasonably and in good faith, and is cooperating diligently to resolve the dispute.

5.3. Taxes

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

6. TERM AND TERMINATION

6.1. Term

The Subscription Term is as stated in the Order Form. If an Order Form indicates for a Cloud Service to qualify as an “Early Ending Item” (“EEI”), the Subscription Term for the EEI will automatically end at the product end date stated in the Order Form for such EEI.

6.2. Termination

A party may terminate:

(a) the Agreement (i) for cause upon 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 30 days of the payment due date) unless the breaching party has cured the breach during such 30 day period; and (ii) immediately if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors, or otherwise materially breaches Sections 111 or 13.6; and

(b) the affected Cloud Service as permitted under Sections 3.4.3, 7.2.4, 7.3.3, 8.1.4, or 13.4 (with termination effective 30 days after receipt of notice in each of these cases).

6.3. Refund and Payments

For termination by Customer (including but not limited to Sections 3.4.3, 6.26.2(a)(i), 7.2.4 or 7.3.3) 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, 100, 111, 122 and 133 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. SAP Warranties and Customer Remedies

7.2.1. Good Industry Warranty

SAP warrants that it will provide the Cloud Service:

(a) in material conformance with the Documentation; and

(b) with the degree of skill and care reasonably expected from a skilled and experienced global supplier of services materially similar to the nature and complexity of the Cloud Service.

7.2.2. Authorization Warranty

Each party warrants that: (a) it is duly organized and validly existing under the laws of the state or country of its incorporation or formation and has full corporate power and authority to enter into and carry out its obligations in this Agreement; (b) this Agreement is enforceable; and (c) the execution, delivery and performance of this Agreement does not conflict with any written agreement to which a party may be bound.

7.2.3. Warranty Against Viruses

SAP warrants that it shall exercise commercially reasonable efforts to keep the Cloud Service, as provided by SAP, free of all viruses, trojan horses, and comparable malicious code intended to harm the Customer's systems, provided, however, SAP shall not be responsible for any malicious code placed on the Cloud Service by Customer, its Authorized Users, or any third party.

7.2.4. 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 3 months of SAP's failure to correct the deficient Cloud Service.

7.3. SAP System Availability Warranty and Customer Remedy

7.3.1. 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").

7.3.2. 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.

7.3.3. In the event SAP fails to meet the SLA (i) for 4 consecutive months, or (ii) for 5 or more months during any 12 month period, or (iii) at a system availability level of at least 95% for 1 calendar month, Customer may terminate its subscriptions for the affected Cloud Service by providing SAP with written notice within 30 days after the failure.

7.4. Warranty Exclusions

The warranties in Sections 7.2 and 7.3 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.

7.5. Disclaimer

Except as expressly provided in the Agreement, neither SAP nor its subcontractors make any representation or warranties, express or implied, statutory or otherwise, regarding any matter, including the merchantability, suitability, originality, or fitness for a particular use or purpose, non-infringement or results to be derived from the use of or integration with any products or services provided under the Agreement, or that the operation of any products or services will be secure, uninterrupted or error free. Customer agrees that it is not relying on delivery of future functionality, public comments or advertising of SAP or product roadmaps in obtaining subscriptions for any Cloud Service.

8. THIRD PARTY CLAIMS

8.1. Claims Brought Against Customer

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. 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 8.3 (b).

(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

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) death or bodily injury arising from either party's gross negligence or willful misconduct; and / or

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

9.2. Liability Cap

Except as set forth in Section 9.1, the maximum aggregate liability of either party (or its respective Affiliates or SAP's subcontractors) to the other or to any other person or entity for all events (or series of connected events) arising in any 12 month period will not exceed the annual subscription fees paid for the applicable Cloud Service associated with the damages for that 12 month period. Any "12 month period" commences on the Subscription Term start date or any of its yearly anniversaries.

9.3. Exclusion of Damages

In no case will:

(a) either party (or its respective Affiliates or SAP's subcontractors) be liable to the other party for any special, incidental, consequential, or indirect damages, loss of goodwill or business profits, work stoppage or for exemplary or punitive damages; and

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

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) 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.

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 111;

(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 111.

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; 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.

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

13.4.1. Each Cloud Service, Documentation and SAP Materials are subject to Export Laws. SAP and Customer shall comply with Export Laws in the performance of the Agreement. Customer, its Affiliates, and Authorized Users shall not directly or indirectly use, export, re-export, release, or transfer the Cloud Service, Documentation and/or SAP Materials in violation of Export Laws. Customer may not permit the use of the Cloud Service, Documentation and/or SAP Materials to any end user with whom transactions are prohibited by Export Laws. Customer, its Affiliates, and Authorized Users shall not access nor use the Cloud Service Documentation and/or SAP Materials and from an embargoed country or region such as Crimea/Sevastopol, Cuba, Iran, the Democratic People's Republic of Korea (North Korea) the so-called Luhansk Peoples Republic (LNR) and Donetsk Peoples Republic (DNR), Syria or any country or region that may violate Export Laws.

13.4.2. Upon SAP's request, Customer shall provide information and documents necessary to support SAP in obtaining an export authorization for the provisioning of the Cloud Service, Documentation and/or SAP Materials. Upon written notice to Customer SAP may terminate Customer's subscription to the affected

Cloud Service if Export Laws prohibit SAP from providing the Cloud Service, Documentation and/or SAP Materials to Customer. Customer is solely responsible for compliance with Export Laws related to Customer Data, including obtaining any required export authorizations for Customer Data.

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

Neither party shall be held responsible (other than for the payment of amounts due hereunder) if the fulfilment of any terms or provisions of this Agreement are delayed or prevented by revolutions or other disorders, wars, acts of enemies, strikes, fires, floods, acts of God, or without limiting the foregoing, by any other cause not within the control of the party whose performance is interfered with, and which exercise of reasonable diligence, the party is unable to prevent, whether of the class of causes herein enumerated or not.

In the event conditions beyond the performing party's reasonable control render the Cloud Service unavailable for more than 30 consecutive days, the other party may terminate the Agreement upon written notice to the performing party (in which case Customer will receive a refund of prepaid unused fees starting from the beginning of the period of unavailability due to such conditions).

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 the State of New York. 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 New York, New York. The parties waive any objections to the venue or jurisdictions identified in this provision. The mandatory, sole and exclusive venue, place or forum for any disputes arising from the Agreement (including any dispute regarding the existence, validity or termination of the Agreement) shall be New York, New York.

13.12. Waiver of Right to Jury Trial

Each party waives any right it may have to a jury trial for any claim or cause of action arising out of or in relation to the Agreement.

13.13. Statute of Limitation

Customer 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 Customer knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

13.14. 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. The Agreement may be modified solely in writing signed by both parties, except as permitted under the Agreement. Terms and conditions of any Customer-issued purchase order shall have no force and effect, even if SAP accepts or does not otherwise reject the purchase order.