

**GENERAL TERMS AND CONDITIONS FOR SAP CLOUD SERVICES (for GSA indirect sales)
("Cloud GTC")**

1. DEFINITIONS

- 1.1. **"Affiliate"** means any legal entity in which SAP SE or Customer, directly or indirectly, holds more than (fifty percent) 50% of the entity's shares or voting rights or controls or is under common control with that legal entity. "Control" means the direct or indirect possession of the power to direct or cause the direction of the management and policies of an entity, whether through ownership, by contract or otherwise. Any 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 Cloud Order Form. For clarity, some services may be performed under a statement of work, which statement of work will be governed by the terms and conditions of this Agreement.
- 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 or suppliers of Customer and its Affiliates.
- 1.5. **"Cloud Order Form"** means the "Cloud Order Form for SAP Cloud Services" concluded between SAP and Reseller that references the Cloud GTC.
- 1.6. **"Cloud Service"** means any distinct, hosted, supported and operated on-demand solution provided by SAP to the Customer on behalf of the Reseller, under the Cloud Order Form.
- 1.7. **"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 or proprietary at the time of disclosure, or should reasonably be understood to be confidential at the time of disclosure given the nature of the information and the circumstances surrounding its disclosure.
- 1.8. **"Customer"** means the entity or individual that has consented to this Agreement by execution of an agreement with Reseller that references this Cloud GTC or by any other legally binding method of acceptance of this Agreement.
- 1.9. **"Customer Data"** means any content, materials, data and information that Authorized Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer-specific reports). Customer Data and its derivatives will not include SAP's Confidential Information.
- 1.10. **"Documentation"** means SAP's then-current technical and functional documentation, relating to the Cloud Services located at <https://help.sap.com> or which is made 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.
- 1.11. **"Export Laws"** means all applicable import, export control and sanctions laws, including without limitation, the laws of the United States, the EU, and Germany.
- 1.12. **"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.
- 1.13. **"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.
- 1.14. **"Reseller"** means the entity holding the Multiple Award Schedule contract and identified on the Cloud Order Form.

- 1.15. **"Representatives"** means a party's Affiliates, employees, contractors, sub-contractors, legal representatives, accountants, or other professional advisors.
- 1.16. **"SAP"** means the entity identified by the Cloud Order Form as providing the Cloud Service to Customer.
- 1.17. **"SAP Materials"** means any materials (including statistical reports) provided, developed or made available by SAP or via Reseller (independently or with Customer's or Reseller's cooperation) in the course of performance under the Agreement, including in the delivery of any support to Customer. SAP Materials do not include Customer Data, Customer Confidential Information or the Cloud Service. SAP Materials may also be referred to in the Agreement as "Cloud Materials".
- 1.18. **"SAP SE"** means SAP SE, the parent company of SAP.
- 1.19. **"Subscription Term"** means the initial subscription term and, if applicable, any renewal subscription term of a Cloud Service identified in the Cloud Order Form.
- 1.20. **"Usage Metric"** means the standard of measurement for determining the permitted use for a Cloud Service as set forth in a Cloud Order Form.

2. USAGE RIGHTS AND RESTRICTIONS

2.1. Grant of Rights

Subject to Reseller's payment of all fees due to SAP, SAP grants to Customer on behalf of Reseller, 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 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 Cloud Order Form. Access credentials for the Cloud Service may not be used by more than one individual, but may be transferred from one individual to another if the original user is no longer permitted to use the Cloud Service. Customer is responsible for breaches of the Agreement caused by Authorized Users.

2.3. Verification of Use

Customer will monitor its own use of the Cloud Service and report any use in excess of the Usage Metrics and volume to Reseller. SAP may monitor use to verify compliance with Usage Metrics, volume and the Agreement. SAP will be permitted to forward any data regarding use in excess of the Usage Metrics, volume and the Agreement by Customer to Reseller. Further, such monitoring shall be contingent upon adherence to Customer's security requirements, including any requirement for personnel to be cleared prior to accessing sensitive IT systems or facilities. If Customer's security requirements are not met, then upon SAP's request, Customer will run a self-assessment with tools provided by, and at the direction of SAP to verify Customer's compliance with the terms of this Agreement.

2.4. 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.

2.5. 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 store. 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.

2.6. On-Premise Components

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

3. SAP RESPONSIBILITIES

3.1. Provisioning

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

3.2. Support

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

3.3. Security

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

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. Any such modifications will not restrict or reduce the capabilities in existence at the time of execution of this Agreement without written concurrence from the Government Contracting Officer.

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 13.4, 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 the Cloud Order Form for the affected Cloud Service by providing written notice to SAP and Reseller within 1 month of SAP's notice. If SAP does not receive timely notice, Customer is deemed to have accepted the modification.

4. CUSTOMER AND PERSONAL DATA

4.1. Customer Ownership

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

4.2. Customer Data

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

4.5.4. In the event of third party legal proceedings relating to Customer Data, SAP will cooperate with Customer and comply with applicable law (both at Customer's expense) with respect to handling of Customer Data.

5. RESELLER RELATIONSHIP, PRICES AND PAYMENT

5.1. Intentionally left blank

5.2. Intentionally left blank

5.3. Independence of Reseller

Reseller is not an agent of SAP. Reseller is an independent entity with no authority to bind SAP or to make representations or warranties on SAP's behalf. SAP will not be liable for reasonably relying on the accuracy and reliability of written information provided by Reseller. Customer acknowledges and agrees that the Reseller through which Customer has arranged for the procurement of the Cloud Services is not an agent of SAP.

5.4. No Representations or Warranties

SAP makes no representations or warranties as to Reseller, any authorized distributor or other reseller, or any other third party, or related to the performance of their products or services, and fully disclaims any such warranties in accordance with Section 7.

5.5. Payment

Customer shall pay to Reseller on behalf of SAP the fees for the Cloud Service provided hereunder, in the amount as set forth in the agreement between Reseller and Customer, in accordance with the terms of the Cloud Order Form.

5.6. Renewal Term

The fees set forth in the Cloud Order Form will be fixed for the committed subscription term. Following the subscription term of a Cloud Order Form, the subscription may be renewed for one (1) year subscription terms (each, as applicable, a "Renewal Term") subject to funding and only for the agreed-upon subscription period by executing a written order for the Renewal Term. Pricing is established based upon the GSA Schedule Price List in effect at the time the Renewal Term is entered into. Either party may give the other party written notice (email acceptable) of non-renewal at least thirty (30) days prior to the end of the relevant subscription term.

5.7. Additions to Cloud Order Form

Customer may add additional Authorized Users or other applicable usage metrics during the term of the Cloud Order Form by executing an addendum or additional schedule with Reseller, as applicable, which shall then become an integral part of the amended Cloud Order Form. The term of each addendum or schedule shall be coterminous with the then-current term of the Cloud Order Form irrespective of the effective date of such addendum and all fees shall be prorated accordingly. Upon renewal of the Cloud Order Form, the term for all Authorized Users or other fee-based metric added to the Cloud Order Form prior to renewal shall be the same as specified in the Cloud Order Form.

5.8. Excess Use

Customer is responsible for monitoring its use of the Service. Customer shall promptly report to SAP any actual use in excess of the number of Authorized Users (or other applicable usage metric authorized in the Cloud Order Form). SAP shall be entitled to monitor Customer's number of Authorized Users (or other applicable usage metric authorized in the Cloud Order Form) regarding usage of the Cloud Service to ensure Customer's compliance with the Agreement. SAP shall be permitted to forward such data to Reseller. SAP shall invoice Reseller and Customer shall have the opportunity to execute an agreement with Reseller to pay for any usage in excess of the usage metrics set forth in the applicable Cloud Order Form. Such fees shall accrue from the date the excess use began. For the avoidance of doubt, Customer shall not be entitled to claim any reduction of the fees payable under the Cloud Order Form or reduce the Authorized Users (or other applicable usage metric) during the term of a Cloud Order Form or renewal.

5.9 No Cancellation

Except as expressly set forth in this Agreement, FAR 52.212-4(l), or the Cloud Order Form, all purchases of subscriptions hereunder are non-cancelable and all fees incurred prior to the termination date are non-refundable.

6. TERM AND TERMINATION

6.1 Term

The term of this Agreement begins on the Effective Date set forth in the applicable Cloud Order Form and shall continue in effect as described in the Cloud Order Form. Termination of individual Cloud Order Forms shall leave other Cloud Order Forms unaffected.

6.2 Termination

Recourse against the United States for any alleged breach of this Agreement must be made under the terms of the Federal Tort Claims Act or as a dispute under the contract disputes clause (Contract Disputes Act, 41 U.S.C. Chapter 71) as applicable. SAP shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Customer. The Agreement shall terminate immediately upon a final judgment obtained under the Contracts Disputes Act terminating the Agreement for Customer's material breach of any provision of the Agreement.

SAP may, in its reasonable determination, deactivate Customer's user name(s) and password(s) and/or temporarily suspend access to the Cloud Service or a portion thereof, if and to the extent SAP can substantiate that the continued use of the Cloud Service may result in harm to the Cloud Service (including the security of the systems used to provide the Cloud Service) or other SAP customers, or the rights of third parties, upon prior written notice to Customer as the circumstances permit.

6.3 Effect of Expiration or Termination

Upon the effective date of termination, Customer's access to the Cloud Service will be terminated. Customer shall have the ability to access its Customer Data at any time during the subscription term set forth in the applicable Order Form, unless earlier terminated pursuant to this Article 6. Customer may export and retrieve its Customer Data during a subscription term, which will be subject to technical limitations caused by factors such as (i) the availability of self-service extraction tools compatible with the Cloud Service, (ii) the size of Customer's instance of the Cloud Service; and (iii) the frequency and/or timing of the export and retrieval.

6.4 Survival

Articles 5, 8, 9, 10, 11, 12 and 13 shall survive the expiration or termination of this 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, Customer Data and Customer's use of the Cloud Service.

7.2. Good Industry Practices

SAP warrants that it will provide the Cloud Service:

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

7.3. Remedy

7.3.1. Provided Customer (or Reseller on Customer's behalf) notifies SAP in writing with a specific description of the Cloud Service's non-conformance with the warranty in Section 7.2 without undue delay and SAP validates the existence of such non-conformance, SAP will, at its option and in accordance with Section 7.3.3:

- (a) correct or replace the non-conforming Cloud Service, or
- (b) if SAP fails to correct the non-conformance after using reasonable commercial efforts, terminate the access to the non-conforming Cloud Service.

7.3.2. The remedies in Section 7.3.1 do not apply to trivial or non-material cases of non-conformance and are Customer's sole and exclusive remedies and SAP's entire liability for breach of the warranty under Section 7.2. The written notification of any non-conformance by Customer (or Reseller on Customer's behalf) must include sufficient detail for SAP to analyze the alleged non-conformance. Customer must provide commercially reasonable assistance to SAP in analyzing and remediating any non-conformance of the Cloud Service.

7.3.3. SAP will consult with Reseller to define a reasonable amount:

- (a) by which Reseller may reduce the subscription fees for the non-conforming Cloud Services, in case Reseller has not already paid them, or
- (b) if Reseller has already paid the subscription fees for the non-conforming Cloud Services, which SAP will refund to Reseller to reflect the non-conformance (unless such refund is prohibited by Export Laws).

7.3.4. SAP may fulfill its warranty obligations with Customer or Reseller on Customer's behalf. To the extent that SAP fulfills its warranty obligations under Section 7.3.3 via Reseller, Customer will not have any claim against SAP for a breach of the warranty in Section 7.2.

7.4. System Availability

7.4.1. 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").

7.4.2. Customer's sole and exclusive remedy for SAP's breach of the SLA is the issuance of a credit as described in the SLA, whereby the service level credit will be calculated based on the non-discounted subscription fee set out in the order form agreed between SAP and Reseller. Customer must notify Reseller in writing (email permitted) within 21 business days after each calendar month in which SAP does not meet the SLA, so that Reseller can follow SAP's posted credit claim procedure. When the validity of the service credit is confirmed by SAP in writing (email permitted) to Reseller, SAP will issue the credit to Reseller to forward to Customer.

7.5. Warranty Exclusions

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

- (a) the Cloud Service is not used in accordance with the Agreement or Documentation;
- (b) any non-conformity is caused by Reseller, Customer, another third party, or by any product, database, content or service not provided by SAP; or
- (c) the Cloud Service was provided for no fee or is a trial license of the Cloud Service.

7.6. Disclaimer

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

delivery of future functionality, public comments or advertising of SAP or product roadmaps in obtaining subscriptions for any Cloud Service.

8. THIRD PARTY CLAIMS

8.1. Claims Brought Against Customer

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) 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.

If these options are not reasonably available, SAP may terminate Customer's subscription to the affected Cloud Service upon written notice.

8.1.4. 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. Customer Responsibilities

Customer shall be responsible for (i) any use of the Cloud Service in violation of any applicable law or regulation; or (ii) an allegation that the Customer Data or Customer's use of the Cloud Service in violation of this Agreement violates, infringes or misappropriates the rights of a third party. The foregoing shall apply regardless of whether such damage is caused by the conduct of Customer and/or its Authorized Users or by the conduct of a third party using Customer's access credentials.

8.3. Conditions

The obligations under this Article 8 are conditioned on (a) the Customer timely notifying SAP in writing of any such claim, provided however that a party's failure to provide or delay in providing such notice shall not relieve a party of its obligations under this Article 8 except to the extent such failure or delay prejudices the defense (b) the party who is obligated hereunder to defend a claim having the right to control the defense of such claim to the extent permitted by 28 U.S.C. §516; and (c) the party against whom a third party claim is brought reasonably cooperating in the defense of such claim. Any settlement of any claim shall not include a financial or specific performance obligation on or admission of liability by the party against whom the claim is brought, provided however that SAP may settle any claim on a basis requiring SAP to substitute for the Cloud Service any alternative substantially equivalent non-infringing services. SAP will have the opportunity to intervene in any suit or claim filed against the Customer, at its own expense, through counsel of its own choosing. Neither party shall undertake any action in response to any infringement or misappropriation, or alleged infringement or misappropriation that is prejudicial to the other party's rights. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

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 Liability

9.1.1. SAP, its licensors or subcontractors will not be responsible or liable under the Agreement:

- (a) if a Cloud Service is not used in accordance with the Documentation;
- (b) if the defect or liability is caused by Reseller, Customer or any third party product or service;
- (c) if the Cloud Service is used in conjunction with any product or service not provided by SAP;
- (d) for any Customer activities not permitted under the Agreement; or
- (e) for any claims or damages arising from inherently dangerous use of any of the Cloud Services provided under or in connection with the Agreement.

9.2. No Cap on Liability

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

- (a) the parties' obligations under Sections 8.1.1 or 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 or any failure by Customer to pay Reseller any fees due for the Cloud Services.

9.3. 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 twelve (12)-month period will not exceed the annual subscription fees paid by Customer to Reseller for the applicable Cloud Service associated with the damages for that twelve (12)-month period. Any "twelve (12)-month period" commences on the Subscription Term start date or any of its yearly anniversaries. NOTWITHSTANDING THE FOREGOING, NOTHING IN THIS SECTION SHALL BE DEEMED TO IMPAIR THE U.S. GOVERNMENT'S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF, OR RELATED TO, THIS AGREEMENT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31 U.S.C. §§ 3729-3733.

9.4. 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.

9.5. Extension to group members

Any limitations to the liability and obligations of SAP according to this Section 9 will also apply for the benefit of SAP SE and any of its Affiliates and their respective licensors.

9.6. SAP will not be obliged to provide an indemnity or damages where Customer has been fully compensated or indemnified for the same loss or damage under its agreement with Reseller.

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 any derivative works of:

- (a) the Cloud Service;
- (b) SAP Materials;
- (c) Documentation; and

- (d) any services, design contributions, related knowledge or processes, whether or not developed for Customer.

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

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 its 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 rights or perform its obligations under the Agreement and who are under obligations of confidentiality substantially similar to those in Section 11;
- (c) not use or reproduce any Confidential Information of the disclosing party for any purpose outside the scope of the Agreement; and
- (d) retain any and all confidential, internal, or proprietary notices or legends which appear on the original and on any reproductions.

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

11.1.3. Confidential Information of either party disclosed prior to execution of the Agreement will be subject to Section 11.

11.2. Compelled Disclosure

The receiving party may disclose the disclosing party's Confidential Information to the extent required by law, regulation, court order or regulatory agency; provided, that the receiving party required to make such a disclosure uses reasonable efforts to give the disclosing party reasonable prior notice of such required disclosure (to the extent legally permitted) and provides reasonable assistance in contesting the required disclosure, at the request and cost of the disclosing party. The receiving party and its Representatives shall use commercially reasonable efforts to disclose only that portion of the Confidential Information which is legally requested to be disclosed and shall request that all Confidential Information that is so disclosed is accorded confidential treatment. Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. § 552, which requires that information that does not fall under certain exceptions must be released when requested and, therefore, some information may be released despite being characterized as "confidential" by the disclosing party.

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

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. No Waiver

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

13.2. Electronic Signature

Electronic signatures that comply with applicable law are deemed original signatures.

13.3. Trade Compliance

13.3.1. SAP and Customer shall comply with Export Laws in the performance of this Agreement. SAP Confidential Information is subject to Export Laws. Customer, its Affiliates, and Authorized Users shall not directly or indirectly export, re-export, release, or transfer Confidential Information in violation of Export Laws. Customer is solely responsible for compliance with Export Laws related to Customer Data, including obtaining any required export authorizations for Customer Data. Customer shall not use the Cloud Service from Crimea/Sevastopol, Cuba, Iran, the People's Republic of Korea (North Korea), the so-called Luhansk Peoples Republic (LNR) and Donetsk Peoples Republic (DNR) or Syria.

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

- (a) the competent authority does not grant such export authorization within 18 months; or
- (b) Export Laws prohibit SAP from providing the Cloud Service to Customer.

13.4. Notices

All notices will be in writing and given when delivered to the address set forth in a Cloud 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.

13.5. Assignment

Customer may not, without SAP's prior written consent, assign, delegate, pledge or otherwise transfer this Agreement, or any of its rights or obligations under this Agreement, or any SAP materials or SAP Confidential Information, to any party, whether voluntarily or by operation of law, including by way of sale of assets, merger or consolidation. Assignment by SAP is subject to FAR 52.232-23 "Assignment of Claims" (May 2014) and FAR subpart 42.12 "Novation and Change-of-Name Agreements."

13.6. Subcontracting

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

13.7. 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.

13.8. Force Majeure

In accordance with GSAR 552.212-4(f), Any delay in performance (other than for the payment of amounts due) caused by conditions beyond the reasonable control of the performing party is not a breach of the Agreement. The time for performance will be extended for a period equal to the duration of the conditions preventing performance.

13.9. Governing Law

This Agreement and any claims arising out of or relating to this Agreement and its subject matter shall be governed by and construed under United States Federal law. Venue and statute of limitations shall be established by applicable Federal law. 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.

13.10. 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.

13.11. Entire Agreement

The Agreement constitutes the complete and exclusive statement of the agreement between SAP and Customer in connection with the parties' business relationship related to the subject matter of the Agreement. All previous representations, discussions, and writings (including any confidentiality agreements) are merged in and superseded by the 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 Section 3.4. This Agreement, however, shall not take precedence over any specific, negotiated terms contained in a Cloud Order Form. 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.

DATA PROCESSING AGREEMENT FOR CLOUD SERVICES

1. DEFINITIONS

- 1.1. **“Controller”** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.
- 1.2. **“Data Protection Law”** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.
- 1.3. **“Data Subject”** means an identified or identifiable natural person as defined by Data Protection Law.
- 1.4. **“EEA”** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.
- 1.5. **“GDPR”** means the General Data Protection Regulation 2016/679.
- 1.6. **“My Trust Center”** means information available on the SAP support portal (see: <https://support.sap.com/en/my-support/trust-center.html>) or the SAP agreements website (see: <https://www.sap.com/about/trust-center/agreements.html>) or any subsequent website(s) made available by SAP to Customer.
- 1.7. **“New SCC Relevant Transfer”** means a transfer (or an onward transfer) to a Third Country of Personal Data that is either subject to GDPR or to applicable Data Protection Law and where any required adequacy means under GDPR or applicable Data Protection Law can be met by entering into the New Standard Contractual Clauses.
- 1.8. **“New Standard Contractual Clauses”** means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof which shall automatically apply. To avoid doubt Modules 2 and 3 shall apply as set out in Section 8.
- 1.9. **“Personal Data”** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is:
 - a) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service; or
 - b) supplied to or accessed by SAP or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).
- 1.10. **“Personal Data Breach”** means a confirmed:
 - a) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data; or
 - b) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.
- 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. **“Schedule”** means the numbered Appendix with respect to the Standard Contractual Clauses (2010) and the numbered Annex with respect to the New Standard Contractual Clauses.
- 1.13. **“Standard Contractual Clauses (2010)”** means the Standard Contractual Clauses (processors) published by the European Commission, reference 2010/87/EU.
- 1.14. **“Subprocessor”** or **“sub-processor”** means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP, SAP SE or SAP SE's Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

1.15. **“Technical and Organizational Measures”** means the technical and organizational measures for the relevant Cloud Service published on My Trust Center (see: <https://www.sap.com/about/trust-center/agreements/cloud/cloud-services.html?search=Technical%20Organizational%20Measures>).

1.16. **“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. Purpose and Application

2.1.1. This document (“**DPA**”) is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer.

2.1.2. This DPA applies to Personal Data processed by SAP and its Subprocessors in connection with its provision of the Cloud Service.

2.1.3. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SAP. Customer shall not store Personal Data in such environments.

2.2. Structure

Schedules 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects (Schedule 1) and the applicable Technical and Organizational Measures (Schedule 2).

2.3. Governance

2.3.1. SAP acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA.

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

2.4. For the avoidance of doubt, nothing in this DPA (including without limitation, Section 1.2 “Data Protection Law”, 1.4 “EEA”, 1.5 “GDPR”, 1.7 “New SCC relevant Transfer”, 1.8 “New Standard Contractual Clauses”, 1.13 “Standard Contractual Clauses (2010)” and Section 1.16 “Third Country” and Section 8, “International Processing” shall be construed as imposing GDPR compliance obligations on Customer in situations where Customer’s use of the SAP Cloud Services would not otherwise subject Customer to GDPR requirements as a Controller.

3. SECURITY OF PROCESSING

3.1. Applicability of the Technical and Organizational Measures

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

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 Cloud Service. SAP may change the Technical and Organizational Measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

- 3.2.2. SAP will publish updated versions of the Technical and Organizational Measures on My Trust Center and where available Customer may subscribe to receive e-mail notification of such updated versions.

4. SAP OBLIGATIONS

4.1. Instructions from Customer

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

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. Cooperation

- 4.4.1. 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.

- 4.4.2. If SAP receives a request from a Data Subject in relation to the Personal Data processing 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.

- 4.4.4. SAP shall provide functionality for production systems 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, SAP will correct, delete or anonymize any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

4.5. 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. Data Protection Impact Assessment

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

5. DATA EXPORT AND DELETION

5.1. Export and Retrieval by Customer

During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case SAP and Customer will find a reasonable method to allow Customer access to Personal Data.

5.2. Deletion

Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs SAP to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed 6 months) unless applicable law requires retention.

6. CERTIFICATIONS AND AUDITS

6.1. Customer Audit

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

- a) SAP has not provided sufficient evidence of its compliance with the Technical and Organizational Measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or SAP;
- b) a Personal Data Breach has occurred;
- c) an audit is formally requested by Customer's data protection authority; or
- d) provided under mandatory Data Protection Law conferring Customer a direct audit right and provided that Customer shall only audit once in any 12 month period unless mandatory Data Protection Law requires more frequent audits.

6.2. Other Controller Audit

Any other Controller may assume Customer's rights under Section 6.1 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer. Customer shall use all reasonable means to combine audits of multiple other Controllers to avoid multiple audits, unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SAP on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

6.3. Scope of Audit

Customer shall provide at least 60 days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of 3 business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to SAP.

6.4. Cost of Audits

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

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 this Agreement;
- b) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and
- c) SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP on My Trust Center or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the Cloud Service.

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 by posting on the My Trust Center) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and
- b) Customer may object to such changes as set out in Section 7.3.

7.3. Objections to New Subprocessors

7.3.1. If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than 30 days from the date of SAP's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this 30 day period, Customer is deemed to have accepted the new Subprocessor.

7.3.2. Within the 30 day period from the date of SAP's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties discuss in good faith a resolution to the objection. Such discussions shall not extend the period for termination and do not affect SAP's right to use the new Subprocessor(s) after the 30 day period.

7.3.3. Any termination under this Section 7.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

7.4. Emergency Replacement

SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 7.2 applies 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. Applicability of the Standard Contractual Clauses (2010)

8.2.1. Where, for the period up to and including 26 September 2021, Personal Data of a Controller that is subject to GDPR is processed in a Third Country, or where Personal Data of a Swiss or United Kingdom based Controller

or another Controller is processed in a Third Country and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses (2010), then:

- a) SAP and Customer enter into the Standard Contractual Clauses (2010);
- b) Customer joins the Standard Contractual Clauses (2010) entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations; or
- c) other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses (2010) with SAP or the relevant Subprocessors in the same manner as Customer in accordance with Section 8.2.1 a) and b) above. In such case, Customer will enter into the Standard Contractual Clauses (2010) on behalf of the other Controllers.

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

8.2.3. Where applicable Data Protection Law adopts the New Standard Contractual Clauses as meeting any required adequacy means as an alternative or update to the Standard Contractual Clauses (2010) then the New Standard Contractual Clauses shall apply in accordance with Section 8.3.

8.3. Applicability of New Standard Contractual Clauses

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

8.3.1.1. Where SAP is not located in a Third Country and acts as a data exporter, SAP (or SAP SE on its behalf) has entered in to the New Standard Contractual Clauses with each Subprocessor as the data importer. Module 3 (Processor to Processor) of the New Standard Contractual Clauses shall apply to such New SCC Relevant Transfers.

8.3.1.2. Where SAP is located in a Third Country:

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

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

8.3.2. Other Controllers or Processors whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into the New Standard Contractual Clauses with SAP in the same manner as Customer in accordance with Section 8.3.1.2.3.1.2 above. In such case, Customer enters into the New Standard Contractual Clauses on behalf of the other Controllers or Processors.

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

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

8.4. Relation of the Standard Contractual Clauses to the Agreement

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

8.5. Third Party Beneficiary Right under the New Standard Contractual Clauses

- 8.5.1. Where Customer is located in a Third Country and acting as a data importer under Module 2 or Module 3 of the New Standard Contractual Clauses and SAP is acting as Customer's sub-processor under the applicable Module, the respective data exporter shall have the following third party beneficiary right:
- 8.5.2. 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 Cloud Service solely to the extent that the data exporter's Personal Data is processed. In such event, the respective data exporter also instructs SAP to erase or return the Personal Data.

9. DOCUMENTATION; RECORDS OF PROCESSING

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

Schedule 1 Description of the Processing

This Schedule 1 applies to describe the Processing of Personal Data for the purposes of the Standard Contractual Clauses (2010), New Standard Contractual Clauses and applicable Data Protection Law.

1. A. LIST OF PARTIES

- 1.1. Under the Standard Contractual Clauses (2010)

- 1.1.1. Data Exporter

The data exporter under the Standard Contractual Clauses (2010) is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also data exporters.

- 1.1.2. Data Importer

SAP and its Subprocessors that provide and support the Cloud Service are data importers under the Standard Contractual Clauses (2010).

- 1.2. Under the New Standard Contractual Clauses

- 1.2.1. Module 2: Transfer Controller to Processor

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

- 1.2.2. Module 3: Transfer Processor to Processor

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

2. B. DESCRIPTION OF TRANSFER

- 2.1. Data Subjects

Unless provided otherwise by the data exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service, transmitted to, made available to, accessed or otherwise processed by the data importer.

- 2.2. Data Categories

The transferred Personal Data concerns the following categories of data:

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

- 2.3. Special Data Categories (if agreed)
 - 2.3.1. The transferred Personal Data may comprise special categories of personal data set out in the Agreement (“**Sensitive Data**”). SAP has taken Technical and Organizational Measures as set out in Schedule 2 to ensure a level of security appropriate to protect also Sensitive Data.
 - 2.3.2. The transfer of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):
 - a) training of personnel;
 - b) encryption of data in transit and at rest;
 - c) system access logging and general data access logging.
 - 2.3.3. In addition, the Cloud Services provide measures for handling of Sensitive Data as described in the Documentation.
- 2.4. Purposes of the data transfer and further processing; Nature of the processing
 - 2.4.1. The transferred Personal Data is subject to the following basic processing activities:
 - a) use of Personal Data to set up, operate, monitor and provide the Cloud Service (including operational and technical support);
 - b) continuous improvement of service features and functionalities provided as part of the Cloud Service including automation, transaction processing and machine learning;
 - c) provision of embedded Professional 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 of Customer in accordance with the Agreement.
 - 2.4.2. The purpose of the transfer 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.
- 2.5. Additional description in respect of the New Standard Contractual Clauses:
 - 2.5.1. Applicable Modules of the New Standard Contractual Clauses
 - a) Module 2: Transfer Controller to Processor
 - b) Module 3: Transfer Processor to Processor
 - 2.5.2. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

In respect of the New Standard Contractual Clauses, transfers to Subprocessors shall be on the same basis as set out in the DPA.

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

Transfers shall be made on a continuous basis.

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

Personal Data shall be retained for the duration of the Agreement and subject to Section 5.2 of the DPA.

3. C. COMPETENT SUPERVISORY AUTHORITY

- 3.1. In respect of the New Standard Contractual Clauses:

- 3.1.1. Module 2: Transfer Controller to Processor

- 3.1.2. Module 3: Transfer Processor to Processor

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

Schedule 2 Technical and Organizational Measures

This Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of the Standard Contractual Clauses (2010), New Standard Contractual Clauses and applicable Data Protection Law.

SAP will apply and maintain the Technical and Organizational Measures.

To the extent that the provisioning of the Cloud Service comprises New SCC Relevant Transfers, the Technical and Organizational Measures set out in Schedule 2 describe the measures and safeguards which have been taken to fully take into consideration the nature of the personal data and the risks involved. If local laws may affect the compliance with the clauses, this may trigger the application of additional safeguards applied during transmission and to the processing of the personal data in the country of destination (if applicable: encryption of data in transit, encryption of data at rest, anonymization, pseudonymization).

DATA PROCESSING AGREEMENT FOR SAP SERVICES ("DPA")

1. DEFINITIONS

- 1.1. **"Audit Reports and Certifications"** mean documents available under: <https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html> or any subsequent website notified to Customer.
- 1.2. **"Cloud Service"** means any distinct, subscription-based, hosted, supported and operated on-demand solution as defined in the Agreement.
- 1.3. **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.
- 1.4. **"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.
- 1.5. **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.
- 1.6. **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.
- 1.7. **"GDPR"** means the General Data Protection Regulation 2016/679.
- 1.8. **"List of Subprocessors"** means a compilation of the name, address and role of each Subprocessor SAP uses to provide SAP Services which is in general published under: <https://support.sap.com/en/my-support/trust-center/subprocessors.html> or any subsequent website notified to Customer.
- 1.9. **"My Trust Center"** means information available on the SAP support portal (see: <https://support.sap.com/en/my-support/trust-center.html>) or the SAP agreements website (see: <https://www.sap.com/about/trust-center/agreements.html>) or any subsequent website(s) made available by SAP to Customer.
- 1.10. **"New SCC Relevant Transfer"** means a transfer (or an onward transfer) to a Third Country of Personal Data that is either subject to GDPR or to applicable Data Protection Law and where any required adequacy means under GDPR or applicable Data Protection Law can be met by entering into the New Standard Contractual Clauses.
- 1.11. **"New Standard Contractual Clauses"** means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof as adopted by SAP. To avoid doubt Modules 2 and 3 shall apply as set out in Section 8.3.
- 1.12. **"Personal Data"** means any information relating to a Data Subject. For the purposes of the DPA, it includes only personal data which is:
 - a) processed by SAP as part of the Cloud Service; or
 - b) supplied to or accessed by SAP or its Subprocessors in order to provide support under the applicable Agreement or in connection with SAP Services.
- 1.13. **"Personal Data Breach"** means cases of a confirmed:
 - a) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data; or
 - b) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.
- 1.14. **"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.
- 1.15. **"SAP Support"** means support services as defined in the applicable Agreement.

- 1.16. **"Schedule"** means the numbered Appendix with respect to the Standard Contractual Clauses (2010) and the numbered Annex with respect to the New Standard Contractual Clauses.
- 1.17. **"Services"** means implementation services, consulting services and/or other related services as defined in the Agreement and may also be referred to in the Agreement as **"Consulting Services"** or **"Professional Services"**.
- 1.18. **"Standard Contractual Clauses (2010)"** means the Standard Contractual Clauses (processors) published by the European Commission, reference 2010/87/EU.
- 1.19. **"Subprocessor"** or **"sub-processor"** means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP, SAP SE or SAP SE's Affiliates in connection with the SAP Services which process Personal Data in accordance with this DPA.
- 1.20. **"Technical and Organizational Measures"** means the technical and organizational measures for the relevant SAP Service published on the My Trust Center (see: <https://www.sap.com/about/trust-center/agreements/cloud/cloud-services.html?search=Technical%20Organizational%20Measures>).
- 1.21. **"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. Application

- 2.1.1. This document ("**DPA**") is incorporated into and forms part of an Agreement between SAP and Customer about SAP Services. For the purpose of this DPA, SAP Services are defined as Cloud Service, Services or SAP Support in the Agreement and are subject to its terms.
- 2.1.2. This DPA sets forth the terms and conditions related to the processing of Personal Data by SAP and its Subprocessors in connection with delivering SAP Services.
- 2.1.3. This DPA does not apply to non-production environments of the SAP Services made available by SAP. Customer shall not store Personal Data in such environments.

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

- 2.4. For the avoidance of doubt, nothing in this DPA (including without limitation, Section 1.4 "Data Protection Law", 1.6 "EEA", 1.7 "GDPR", 1.10 "New SCC relevant Transfer", 1.11 "New Standard Contractual Clauses", 1.18 "Standard Contractual Clauses (2010)" and Section 1.21 "Third Country" and Section 8, "International Processing" shall be construed as imposing GDPR compliance obligations on Customer in situations where Customer's use of the SAP Cloud Services would not otherwise subject Customer to GDPR requirements as a Controller.

3. SECURITY OF PROCESSING

3.1. Applicability of the 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 the Technical and Organizational Measures as necessary and may change the Technical and Organizational Measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3.2.2. SAP will publish updated versions of the Technical and Organizational Measures on My Trust Center and where available Customer may subscribe to receive e-mail notification of such updated versions.

4. OBLIGATIONS

4.1. Instructions from Customer

SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented instructions. SAP will use reasonable efforts to follow any additional reasonable Customer instructions, as long as technically feasible. If SAP will not comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (e-mail permitted).

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. Cooperation

4.4.1. 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 processing 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.

4.4.2. 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.

4.4.3. SAP shall provide functionality for production systems 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, SAP will correct, delete or anonymize any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

4.5. 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. Data Protection Impact Assessment

If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SAP will provide such

documents as are generally available for the SAP Services (for example, this DPA, the Agreement, Audit Reports and Certifications). Any additional assistance shall be mutually agreed between the Parties.

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 can access its Personal Data at any time. Customer may use SAP's self-service export tools and retrieve its Personal Data in a structured, commonly used and machine-readable format.

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. SAP Resources

SAP provides Audit Reports and Certifications free of charge, online or upon request. Additional verifications that require SAP resources are limited and subject to the following Sections.

6.2. Limitations

6.2.1. Customer or its independent third party auditor (reasonably acceptable to SAP excluding any third party auditor who is either a competitor of SAP or not suitably qualified) may be permitted to conduct an audit under Sections 6.3 and 6.4. Customer shall provide at least 60 days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice.

6.2.2. The frequency (not to exceed once every 12 months), timeframe and scope of any audit shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited to remote audits where possible. Customer shall provide the results of any audit to SAP. Customer shall bear the 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. Cloud Services Customer Audit

6.3.1. Customer may audit SAP's control environment and IT security practices relevant to Personal Data processed by SAP, that require SAP resources equivalent to a maximum of 3 business days if:

- a) SAP has not provided sufficient evidence of its compliance with the Technical and Organizational Measures through providing a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate), such as a valid SSAE18/ISAE3402 and/or ISAE3000 (e.g. SOC2 or C5) or an equally accepted regional or local certification or attestation; or
- b) a Personal Data Breach has occurred; or
- c) an audit is formally requested by Customer's data protection authority or provided under mandatory Data Protection Law.

6.4. SAP Support and Services Customer Audit

Customer may audit SAP's service and support delivery centers and IT security practices relevant to Personal Data processed by SAP that require SAP resources equivalent to a maximum of 1 business day if:

- a) SAP has not provided sufficient evidence of its compliance with the Technical and Organizational Measures through providing a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or
- b) a Personal Data Breach has occurred; or
- c) an audit is formally requested by Customer's data protection authority or provided under mandatory Data Protection Law.

6.5. Other Controller Audit

Any other Controller may assume Customer's rights under this Section 6 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer. Customer shall use all reasonable means to combine audits of multiple other Controllers 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 including name, address and role of the new Subprocessor. Customer agrees to register on the My Trust Center and subscribe to its applicable and available List of Subprocessors. If Customer does not object, Customer is deemed to have accepted the new Subprocessor.
- b) Customer may object to a new Subprocessor by notifying SAP in writing within 5 business days of SAP's information for Services and in case of SAP Support and Cloud Services within 30 calendar days and explaining the reasonable ground(s) for its objection.
- c) If Customer objects SAP may choose: (i) not to use the Subprocessor; or (ii) to take reasonable measures to remedy Customer's grounds for its objection and use the Subprocessor or (iii) if this is not possible, use the Subprocessor. If Customer continues to have a legitimate objection, Customer may only terminate the affected SAP Service using the new Subprocessor, however termination of SAP Support shall also comply with the termination provision of the respective SAP Support agreement. Such termination shall take effect at the time determined by the Customer in its written termination notice provided Customer accepts the use of the proposed Subprocessor during the remainder of the Agreement 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 any 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

SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 7.2 applies 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. Applicability of the Standard Contractual Clauses (2010)

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

- a) if applicable, SAP and Customer enter into the Standard Contractual Clauses (2010);
- b) Customer joins the Standard Contractual Clauses (2010) entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations; or
- c) other Controllers whose use of the SAP Services have been authorized by Customer under the applicable Agreement may also enter into Standard Contractual Clauses (2010) with SAP or the relevant Subprocessors in the same manner as Customer in accordance with Sections 8.2.1 (a) and (b) above.

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

8.2.3. Where applicable Data Protection Law adopts the New Standard Contractual Clauses as meeting any required adequacy means as an alternative or update to the Standard Contractual Clauses (2010) then the New Standard Contractual Clauses shall apply in accordance with Section 8.3.

8.3. Applicability of New Standard Contractual Clauses

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

8.3.1.1. Where SAP is not located in a Third Country and acts as a data exporter, SAP (or SAP SE on its behalf) has entered into the New Standard Contractual Clauses with each Subprocessor as the data importer. Module 3 (Processor to Processor) of the New Standard Contractual Clauses shall apply to such New SCC Relevant Transfers.

8.3.1.2. Where SAP is located in a Third Country:

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

- 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 act as Processor under Module 3 (Processor to Processor) of the New Standard Contractual Clauses, SAP acknowledges that Customer acts as Processor under the instructions of its Controller(s).

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

- 8.3.2. With respect to a New SCC Relevant Transfer, on request from a Data Subject to the Customer, Customer may make a copy of Module 2 or 3 of the New Standard Contractual Clauses entered into between Customer and SAP (including the relevant Schedules), available to Data Subjects.
- 8.3.3. The governing law of the New Standard Contractual Clauses shall be the law of Germany.
- 8.4. Relation of the Standard Contractual Clauses to the Agreement

Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses (2010) or the New Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and Subprocessor rules, such specifications also apply in relation to the Standard Contractual Clauses (2010) and the New Standard Contractual Clauses.
- 8.5. Third Party Beneficiary Right under the New Standard Contractual Clauses
 - 8.5.1. Where Customer is located in a Third Country and acting as a data importer under Module 2 or Module 3 of the New Standard Contractual Clauses and SAP is acting as Customer's sub-processor under the applicable Module, the respective data exporter shall have the following third party beneficiary right:
 - 8.5.2. In the event that Customer has factually disappeared, ceased to exist in law or has become insolvent (in all cases without as 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.

9. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements. Customer shall provide and maintain information on all Controllers (e.g. legal name and address) using the SAP Services in electronic format (e.g. in the Order Form) as reasonably requested by SAP, in order to enable SAP to comply with any obligations relating to maintaining records of processing.

Schedule 1 Description of the Processing

This Schedule 1 applies to describe the Processing of Personal Data for the purposes of the Standard Contractual Clauses (2010), New Standard Contractual Clauses and applicable Data Protection Law.

1. A. LIST OF PARTIES

1.1. Under the Standard Contractual Clauses (2010)

1.1.1. Data Exporter

The data exporter is the Customer who has concluded the Agreement with SAP for the provision of SAP Services as further described under the relevant Agreement. The data exporter allows other Controllers to also use the SAP Service, these other Controllers are also data exporters.

1.1.2. Data Importer

1.1.2.1. In respect of Cloud Services

SAP and its Subprocessors that provide and support the Cloud Service are data importers under the Standard Contractual Clauses (2010).

1.1.2.2. In respect of other SAP Services

SAP and its Subprocessors provide the SAP Service as defined under the relevant Agreement concluded by the data exporter that includes Standard Contractual Clauses (2010) are data importers.

1.2. Under the New Standard Contractual Clauses

1.2.1. Module 2: Transfer Controller to Processor

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

1.2.2. Module 3: Transfer Processor to Processor

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

2. B. DESCRIPTION OF TRANSFER

2.1. Data Subjects

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

2.2. Data Categories

The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data and/or data fields which could be transferred per SAP Service as stated in the relevant Agreement. For Cloud Services, Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, 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.

2.3. Special Data Categories (if agreed)

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

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

- a) training of personnel;
- b) encryption of data in transit and at rest ;
- c) system access logging and general data access logging.

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

2.4. Purposes of the data transfer and further processing; Nature of the processing

2.4.1. For Cloud Services

2.4.1.1. The transferred Personal Data is subject to the following basic processing activities:

- a) use of Personal Data to set up, operate, monitor and provide the Cloud Service (including operational and technical Support);
- b) continuous improvement of service features and functionalities provided as part of the Cloud Service including automation, transaction processing and machine learning;
- c) provision of 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 of Customer in accordance with the Agreement.
- 2.4.1.2. The purpose of the transfer 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.
- 2.4.2. For other SAP Services
- The transferred 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 Services;
 - b) use of Personal Data to provide 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;
 - f) execution of instructions of Customer in accordance with the Agreement;
- 2.4.3. 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. They answer phone calls and perform basic troubleshooting, and handle support tickets in a tracking system.
- 2.4.4. For Services: SAP or its Subprocessors provide Services subject to the Order Form Services and the applicable Scope Document.
- 2.5. 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.
- 2.6. 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.
- 2.7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
- Personal Data will be retained by SAP as set out in Section 5 above.
- 2.8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:
- SAP will transfer Personal Data to Subprocessors as stated in the applicable List of Subprocessors for the duration of the Agreement.
- 3. C. COMPETENT SUPERVISORY AUTHORITY**
- 3.1. In respect of the New Standard Contractual Clauses:
- 3.1.1. Module 2: Transfer Controller to Processor
 - 3.1.2. Module 3: Transfer Processor to Processor
- 3.2. Where Customer is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the New Standard Contractual Clauses.

Schedule 2 Technical and Organizational Measures

This Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of the Standard Contractual Clauses (2010), New Standard Contractual Clauses and applicable Data Protection Law.

SAP will apply and maintain the Technical and Organizational Measures.

To the extent that the provisioning of the Cloud Service comprises New SCC Relevant Transfers, the Technical and Organizational Measures set out in Schedule 2 describe the measures and safeguards which have been taken to fully take into consideration the nature of the personal data and the risks involved. If local laws may affect the compliance with the clauses, this may trigger the application of additional safeguards applied during transmission and to the processing of the personal data in the country of destination (if applicable: encryption of data in transit, encryption of data at rest, anonymization, pseudonymization).