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

1. DEFINITIONS

Capitalized terms used in this document are defined in the Glossary at the end of this document.

2. USAGE RIGHTS AND RESTRICTIONS

2.1 Grant of Rights.

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

2.2 Authorized Users.

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

2.3 Acceptable Use Policy.

With respect to the Cloud Service, Customer will not:

(a) except to the extent such rights cannot be validly waived by law, disassemble, decompile, reverse-engineer, copy, translate or make derivative works,

(b) transmit any content or data that is unlawful or infringes any intellectual property rights, or

(c) circumvent or endanger its operation or security.

2.4 Verification of Use.

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

2.5 Suspension of Cloud Service.

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

2.6 Third Party Web Services.

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

2.7 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.

2.8 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. In addition to the support policy referenced in the Order Form, specific SAP support and maintenance policies apply to the On-Premise Components and can be found in SAP Support Note 2658835.

3. SAP RESPONSIBILITIES

3.1 Provisioning.

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

3.2 Support.

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

3.3 Security.

SAP 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 for SAP Cloud Services incorporated into the Order Form in compliance with applicable data protection law.

3.4 Modifications.

(a) The Cloud Service and SAP Policies may be modified by SAP. SAP will inform Customer of modifications by email, the support portal, release notes, Documentation or the Cloud Service. The information will be delivered by email if the modification is not solely an enhancement. Modifications may include optional new features for the Cloud Service, which Customer may use subject to the then-current Supplement and Documentation.

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

3.5 Analyses.

SAP, SAP SE or SAP Affiliates may create analyses utilizing, in part, Customer Data and information derived from Customer's use of the Cloud Service and Consulting Services, as set forth below ("**Analyses**"). Analyses will anonymize and aggregate information and will be treated as Cloud Materials. Unless otherwise agreed, personal data contained in Customer Data is only used to provide the Cloud Service and Consulting Services. Analyses may be used for the following purposes:

a) product improvement (in particular, product features and functionality, workflows and user interfaces) and development of new SAP products and services,
b) improving resource allocation and support,
c) internal demand planning,
d) training and developing machine learning algorithms,
e) improving product performance,
f) verification of security and data integrity,
g) identification of industry trends and developments, creation of indices and anonymous benchmarking.

4. CUSTOMER AND PERSONAL DATA

4.1 Customer Data.

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

4.2 Personal Data.

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

4.3 Security.

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

4.4 Access to Customer Data.

(a) During the Subscription Term, Customer can access its Customer Data at any time. Customer may export and retrieve its Customer Data in a standard format. Export and retrieval may

be subject to technical limitations, in which case SAP and Customer will find a reasonable method to allow Customer access to Customer Data.

(b) Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Customer Data from the Cloud Service.

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

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

5. FEES AND TAXES

5.1 Fees and Payment.

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

5.2 Taxes.

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

6. TERM AND TERMINATION

6.1 Term.

The Subscription Term is as stated in the Order Form.

6.2 Termination.

A party may terminate the Agreement:

(a) upon thirty days written notice of the other party's material breach unless the breach is cured during that thirty day period,

(b) as permitted under Sections 3.4(b), 7.3(b), 7.4(c), or 8.1(c) (with termination effective thirty days after receipt of notice in each of these cases), or

(c) immediately if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors, or otherwise materially breaches Sections 11 or 12.6.

6.3 Refund and Payments.

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

(a) a pro-rata refund in the amount of the unused portion of prepaid fees for the terminated subscription calculated as of the effective date of termination, and

(b) a release from the obligation to pay fees due for periods after the effective date of termination.

6.4 Effect of Expiration or Termination.

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

(a) Customer's right to use the Cloud Service and all SAP Confidential Information will end,

(b) Confidential Information of the disclosing party will be returned or destroyed as required by the Agreement, and

(c) termination or expiration of the Agreement does not affect other agreements between the parties.

6.5 Survival.

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

7. WARRANTIES

7.1 Compliance with Law.

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

(a) in the case of SAP, the operation of SAP's business as it relates to the Cloud Service, and

(b) in the case of Customer, the Customer Data and Customer's use of the Cloud Service.

7.2 Good Industry Practices.

SAP warrants that it will provide the Cloud Service:

(a) in substantial conformance with the Documentation; and

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

7.3 Remedy.

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

(a) the re-performance of the deficient Cloud Service, and

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

7.4 System Availability.

(a) SAP warrants to maintain an average monthly system availability for the production system of the Cloud Service as defined in the applicable service level agreement or Supplement ("SLA").

(b) Customer's sole and exclusive remedy for SAP's breach of the SLA is the issuance of a credit in the amount described in the SLA. Customer will follow SAP's posted credit claim procedure. When the validity of the service credit is confirmed by SAP in writing (email permitted), Customer may apply the credit to a future invoice for the Cloud Service or request a refund for the amount of the credit if no future invoice is due.

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

7.5 Warranty Exclusions.

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

(a) the Cloud Service is not used in accordance with the Agreement or Documentation,

(b) any non-conformity is caused by Customer, or by any product or service not provided by SAP, or

(c) the Cloud Service was provided for no fee.

7.6 Disclaimer.

Except as expressly provided in the Agreement, neither SAP nor its subcontractors make any representation or warranties, and SAP and its subcontractors disclaim all representations, warranties, terms, conditions or statements, which might have effect between the parties or be implied or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded to the fullest extent permitted by law including the implied conditions, warranties or other terms as to merchantability, suitability, originality, or fitness for a particular use or purpose. Further, except as expressly provided in this Agreement, neither SAP nor its subcontractors make any representations, warranties, terms, conditions or statements of non-infringement or results to be derived from the use of or integration with any products or services provided under the Agreement, or that the operation of any products or services will be secure, uninterrupted or error free. Customer agrees that it is not relying on delivery of future functionality, public comments or advertising of SAP or product roadmaps in obtaining subscriptions for any Cloud Service.

8. THIRD PARTY CLAIMS

8.1 Claims Brought Against Customer.

(a) SAP will defend Customer against claims brought against Customer and its Affiliates by any third party alleging that Customer's and its Affiliates' use of the Cloud Service infringes or misappropriates a patent claim, copyright, or trade secret right belonging to such third party. SAP will indemnify Customer against all damages finally awarded against Customer (or the amount of any settlement SAP enters into) with respect to these claims.

(b) SAP's obligations under Section 8.1 will not apply if the claim results from (i) Customer's breach of Section 2, (ii) use of the Cloud Service in conjunction with any product or service not provided by SAP, or (iii) use of the Cloud Service provided for no fee.

(c) In the event a claim is made or likely to be made, SAP may (i) procure for Customer the right to continue using the Cloud Service under the terms of the Agreement, or (ii) replace or modify the Cloud Service to be non-infringing without a material decrease in functionality. If these options are not reasonably available, SAP or Customer may terminate Customer's subscription to the affected Cloud Service upon written notice to the other.

8.2 Claims Brought Against SAP.

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

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

8.3 Third Party Claim Procedure.

(a) The party against whom a third party claim is brought will timely notify the other party in writing of any claim, reasonably cooperate in the defense and may appear (at its own expense) through counsel reasonably acceptable to the party providing the defense.

(b) The party that is obligated to defend a claim will have the right to fully control the defense.

(c) Any settlement of a claim will not include a financial or specific performance obligation on, or admission of liability by, the party against whom the claim is brought.

8.4 Exclusive Remedy.

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

9. LIMITATION OF LIABILITY

9.1 Unlimited Liability.

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

(a) the parties' obligations under Section 8.1(a) and 8.2,

(b) unauthorized use or disclosure of Confidential Information,

(c) either party's breach of its data protection and security obligations that result in an unauthorized use or disclosure of personal data,

(d) breach of the obligations imposed by s.12, Sales of Goods Act 1979 or s.2, Supply of Goods and Services Act 1982,

(e) fraud or fraudulent misrepresentation,

(f) death or bodily injury arising from either party's negligence or willful misconduct,

(g) any failure by Customer to pay any fees due under the Agreement, or

(h) any liability that cannot be excluded or limited by applicable law.

9.2 Liability Cap.

Subject to Sections 9.1 and 9.3, and regardless of the basis of liability (whether arising out of liability under breach of contract, tort (including but not limited to negligence), misrepresentation, breach of statutory duty, breach of warranty, claims by third parties arising from any breach of this Agreement), the maximum aggregate liability of either party (or its

respective Affiliates or SAP's subcontractors) arising out of this Agreement to the other or any other person or entity for all events (or series of connected events) arising in any twelve month period will not exceed the annual subscription fees paid for the applicable Cloud Service directly causing the damage for that twelve month period. Any "twelve month period" commences on the Subscription Term start date or any of its yearly anniversaries.

9.3 Exclusion of Damages.

Subject to Section 9.1:

(a) Regardless of the basis of liability (whether arising out of liability under breach of contract, tort (including but not limited to negligence), misrepresentation, breach of statutory duty, breach of warranty, claims by third parties arising from any breach of this Agreement), under no circumstances shall either party (or their respective Affiliates or SAP's subcontractors) be liable to the other party or any third party for any loss or damage (whether or not the other party had been advised of the possibility of such loss or damage) in any amount, to the extent that such loss or damage is (i) consequential, indirect, exemplary, special or punitive; or (ii) for any loss of profits, loss of business, loss of business opportunity, loss of goodwill, loss resulting from work stoppage, or loss of revenue or anticipated savings, whether any such loss or damage is direct or indirect, and

(b) SAP will not be liable for any damages caused by any Cloud Service provided for no fee.

9.4 Risk Allocation.

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

10. INTELLECTUAL PROPERTY RIGHTS

10.1 SAP Ownership.

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

10.2 Customer Ownership.

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

10.3 Non-Assertion of Rights.

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

11. CONFIDENTIALITY

11.1 Use of Confidential Information.

(a) The receiving party will protect all Confidential Information of the disclosing party as strictly confidential to the same extent it protects its own Confidential Information, and not less than a reasonable standard of care. Receiving party will not disclose any Confidential Information of the disclosing party to any person other than its personnel, representatives or Authorized Users whose access is necessary to enable it to exercise its rights or perform its obligations under the Agreement and who are under obligations of confidentiality substantially similar to those in Section 11. Customer will not disclose the Agreement or the pricing to any third party.

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

(c) In the event of legal proceedings relating to the Confidential Information, the receiving party will cooperate with the disclosing party and comply with applicable law (all at disclosing party's expense) with respect to handling of the Confidential Information.

11.2 Exceptions.

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

(a) is independently developed by the receiving party without reference to the disclosing party's Confidential Information,

(b) is generally available to the public without breach of the Agreement by the receiving party,

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

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

11.3 Publicity.

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

12. MISCELLANEOUS

12.1 Severability.

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

12.2 No Waiver.

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

12.3 Electronic Signature.

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

12.4 Regulatory Matters.

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

12.5 Notices.

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

12.6 Assignment.

Without SAP's prior written consent, Customer may not assign or transfer the Agreement (or any of its rights or obligations) to any party. SAP may assign the Agreement to SAP SE or any of its Affiliates.

12.7 Subcontracting.

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

12.8 Relationship of the Parties.

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

12.9 Force Majeure.

Any delay in performance (other than for the payment of amounts due) caused by conditions beyond the reasonable control of the performing party is not a breach of the Agreement. The

time for performance will be extended for a period equal to the duration of the conditions preventing performance.

12.10 Governing Law.

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

12.11 Entire Agreement.

The Agreement constitutes the complete and exclusive statement of the agreement between SAP and Customer relating to the subject matter hereof and supersedes all prior agreements, arrangements and understandings between the parties relating to that subject matter. Each party acknowledges that in entering into the Agreement it has not relied on any representation, discussion, collateral contract or other assurance except those expressly set out in the Agreement. Each party waives all rights and remedies which, but for this section, might otherwise be available to it in respect of any such representation, discussion, collateral contract or other assurance. Except as permitted under Section 3.4, this Agreement may be modified only by a writing signed by both parties. The Agreement shall prevail over any additional, conflicting, or inconsistent terms and conditions which may appear on any purchase order furnished by one party to the other, and any additional terms and conditions in any such purchase order shall have no force and effect, notwithstanding the non-furnishing party's acceptance or execution of such purchase order.

12.12 Contracts Rights of Third Parties.

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

Glossary

1.1 **"Affiliate"** of a party means any legal entity in which a party, directly or indirectly, holds more than fifty percent (50%) of the entity's shares or voting rights. Any legal entity will be considered an Affiliate as long as that interest is maintained.

1.2 **"Agreement"** means an Order Form and documents incorporated into an Order Form.

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

(a) Customer,
(b) Customer's Affiliates, and/or
(c) Customer's and Customer's Affiliates' Business Partners.

1.4 **"Business Partner"** means a legal entity that requires use of a Cloud Service in connection with Customer's and its Affiliates' internal business operations. These may include customers, distributors, service providers and/or suppliers of Customer.

1.5 **"Cloud Service"** means any distinct, subscription-based, hosted, supported and operated on-demand solution provided by SAP under an Order Form.

1.6 **"Cloud Materials"** mean any materials provided or developed by SAP (independently or with Customer's cooperation) in the course of performance under the Agreement, including in the delivery of any support or Consulting Services to Customer. Cloud Materials do not include the Customer Data, Customer Confidential Information or the Cloud Service.

1.7 **"Confidential Information"** means

(a) with respect to Customer: (i) the Customer Data, (ii) Customer marketing and business requirements, (iii) Customer implementation plans, and/or (iv) Customer financial information, and
(b) with respect to SAP: (i) the Cloud Service, Documentation, Cloud Materials and analyses under Section 3.5, and (ii) information regarding SAP research and development, product offerings, pricing and availability.
(c) Confidential Information of either SAP or Customer also includes information which the disclosing party protects against unrestricted disclosure to others that (i) the disclosing party or its representatives designates as confidential at the time of disclosure, or (ii) should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding its disclosure.

1.8 **"Consulting Services"** means professional services, such as implementation, configuration, custom development and training, performed by SAP's employees or subcontractors as described in any Order Form and which are governed by the Supplement for Consulting Services or similar agreement.

1.9 **"Customer Data"** means any content, materials, data and information that Authorized Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer-specific reports). Customer Data and its derivatives will not include SAP's Confidential Information.

1.10 **"Documentation"** means SAP's then-current technical and functional documentation as well as any roles and responsibilities descriptions, if applicable, for the Cloud Service which is made available to Customer with the Cloud Service.

1.11 **"Order Form"** means the ordering document for a Cloud Service that references the GTC.

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

1.13 **"SAP Policies"** means the operational guidelines and policies applied by SAP to provide and support the Cloud Service as incorporated in an Order Form.

1.14 **"Subscription Term"** means the term of a Cloud Service subscription identified in the applicable Order Form, including all renewals.

1.15 **"Supplement"** means the supplemental terms and conditions that apply to the Cloud Service and that are incorporated in an Order Form.

1.16 **"Usage Metric"** means the standard of measurement for determining the permitted use and calculating the fees due for a Cloud Service as set forth in an Order Form.

PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

1. BACKGROUND

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

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

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

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

2. SECURITY OF PROCESSING

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

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

3. SAP OBLIGATIONS

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

with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted).

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

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

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

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

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

4. DATA EXPORT AND DELETION

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

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

5. CERTIFICATIONS AND AUDITS

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

(a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards

(scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or SAP;

(b) A Personal Data Breach has occurred;

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

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

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

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

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

6. SUBPROCESSORS

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

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

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

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

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

(a) SAP will inform Customer in advance (by email or by posting on the support portal available through SAP Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

(b) Customer may object to such changes as set out in Section 6.3.

6.3 Objections to New Subprocessors.

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SAP's notice to Customer

informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.

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

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

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

7. INTERNATIONAL PROCESSING

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

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

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

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

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

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

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

8. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such

as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

9. EU ACCESS

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

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

9.3 **Data Center Location.** Upon the effective date of the Agreement, the Data Centers used to host Personal Data in the Cloud Service are located in the EEA or Switzerland. SAP will not migrate the Customer instance to a Data Center outside the EEA or Switzerland without Customer's prior written consent (email permitted). If SAP plans to migrate the Customer instance to a Data Center within the EEA or to Switzerland, SAP will notify Customer in writing (email permitted) no later than thirty days before the planned migration.

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

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

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

10. DEFINITIONS

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

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

10.2 **"Data Center"** means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as published at: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html or notified to Customer or otherwise agreed in an Order Form.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement.

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

This Appendix 2 comprises two sets of technical and organizational measures ("**TOMs**"):

- **TOMs Set 1 (last updated April 2018, without change):** applies to all Cloud Services, except for the TOMs Set 2 Services defined below.

- **TOMs Set 2**: applies to the TOMs Set 2 Services only. As of July 1, 2020, "**TOMs Set 2 Services**" means the following Cloud Services: SAP Analytics Cloud. SAP may remove a Cloud Service from the list of TOMs Set 2 Services from time to time, in which case such Cloud Service will be subject to TOMs Set 1.

TOMs SET 1

Last Updated: April 2018

1. TECHNICAL AND ORGANIZATIONAL MEASURES

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

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

Measures:

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.

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

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy
- All personnel access SAP's systems with a unique identifier (user ID).
- SAP has procedures in place so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.
- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

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

Measures:

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

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

Measures:

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.

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

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems.
Measures:
- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.

1.6 Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.
Measures:
- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

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

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

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

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

Measures:

- SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
- In particular, SAP uses the following to implement the control and measure sections described above:
- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

TOMs SET 2

(*applies to TOMs Set 2 Services defined above*)

Last Updated: May 4, 2020

1. TECHNICAL AND ORGANIZATIONAL MEASURES

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

1.1 Physical Access Control.

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.

1.2 System Access Control.

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy.
- All personnel access SAP's systems with a unique identifier (user ID).
- SAP has policies designed to provide that no rights are granted without authorization and in case personnel leaves the company their access rights are revoked.
- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

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

1.3 Data Access Control.

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfil their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and/or penetration tests on its IT systems.
- Processes and policies to detect the installation of unapproved software on production systems.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control.

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

1.5 Data Input Control.

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

1.6 Job Control.

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

1.7 Availability Control.

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

1.8 Data Separation Control.

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

1.9 Data Integrity Control.

- SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
- In particular, SAP uses the following to implement the control and measure sections described above.
- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing and/or regular external audits to prove security measures.

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

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

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