SAP SERVICES

General Terms and Conditions

SAP Deutschland SE & Co. KG

(“Services GTC”)

APPLICABILITY

Except in respect of the provision, licensed use, and maintenance of standard software, these present General Terms and Conditions and the provisions of the SAP Services Germany Pricing and Conditions List (herein: “Services PCL”) apply exclusively to every Order Form (see section 1.8) by which SAP provides Services for another business person or public-law juristic person or special fund (herein: Customer).

The provisions of the Software Agreement in the meaning of section 1.10 herein or the Cloud Service Order Form apply conclusively to the provision, licensed use, and maintenance of standard software and/or access to SAP Cloud Services.

No conflicting or other conditions, especially Customer’s general terms and conditions, form any part of the Order Form, even where SAP has performed an Order Form without expressly rejecting such conditions. If, for reasons related to Customer’s technical arrangements or otherwise, Customer’s conditions of purchase or other standard terms are included by insertion, reference, enclosure, attachment or otherwise in Customer’s acceptance of SAP’s offer (for example, in Customer’s purchase order), Customer cannot rely on those conditions or terms and they are not incorporated in and do not form any part of the Order Form, and failure to expressly exclude them does not imply their acceptance.

1. DEFINITIONS

1.1 “Affiliate” means any legal entity that is affiliated with another company within the meaning of the German Stock Corporation Act (AktG), section 15

1.2 “Confidential Information” means all information which SAP or Customer protects against unrestricted disclosure to others, or that are deemed confidential according to the circumstances of their disclosure or their content. In any case, the following information is considered to be Confidential Information of SAP: the SAP Software, programs, tools, data and other material, that SAP provides to Customer before or on the basis of the Order Form.

1.3 “Contract Works” means all the results of the Services provided by SAP in the course of the respective Order Form.

1.4 “Customer Data” means any content, materials, data and information that Customer enters into in a by SAP provided system Customer-specific data that is derived from Customer’s use of the by SAP provided system. Customer Data shall not include any component of Services.

1.5 “Consultant” means SAP employees and subcontractors of SAP including self-employed persons deployed by SAP to perform its contractual duties or processing the Services.

1.6 “IP Rights” (“Intellectual Property Rights”) means any and every patent or other title to or right in an invention, copyright, right of authorship, mark, design, or other industrial right, and all rights to exploit or use it.

1.7 “Order Form” means the agreements on the provision of Services. It may be referred as “Contract” .

1.8 “Services” mean all those Services, that SAP in the meaning of section “Applicability” paragraph 1 makes part of this Services GTC, that are described in an Order Form and/or thereto attached “Service Description” and/or “Scope Document”.

1.9 “SAP Software” means (i) any and all standard software products (as well as relevant documentation) all as developed by or for SAP or any of its affiliated companies; (ii) any new versions (especially without being limited to releases, updates, patches, corrections) thereof made available pursuant to the Software Agreement; and (iii) any complete or partial copies of any of the foregoing.

1.10 “Software Agreement” means the agreements on the license and support of standard software or SAP Cloud Service between SAP (or an affiliate or of SAP SE within the meaning of the German Stock Corporation Act, sections 15 ff or an authorized partner of SAP) and Customer that grant Customer the right to use SAP Software or SAP Cloud Service.

2. PROVISION OF SERVICES

2.1 Customer must describe the requirements for the Services. On the basis of that description, SAP and Customer must plan the provision of Services together. SAP can, if necessary, submit a written concept for that purpose. Further details will be set out or referenced in the Order Form.

2.2 SAP will decide which Consultant to deploy and reserves the right to replace any Consultant at any time. SAP is liable for faults committed by another in performance of a contractual duty of SAP on SAP’s behalf (an “Erfüllungsgehilfe”) to the same extent as SAP is liable for its own such faults. The Services can be provided at SAP´s discretion either in the business offices of SAP, at the Customer´s place of business or remote. Even where Services are provided at Customer’s facility, SAP has sole managerial authority over its Consultants. The Consultants do not become integrated into Customer’s workforce. Customer can issue instructions only to SAP’s project coordinator, and not directly to individual SAP Consultants.

2.3 Customer bears the risk of ordered Services meeting Customer’s wishes and needs. If in doubt, Customer should obtain advice from employees of SAP or third-party experts in good time. Customer has to examine, if Customer is required to license further or other licenses, resulting from the completion of the project. SAP expressly informs Costumer that SAP did not examine the requirement of further or other licenses and that this is not within the scope of the Order Form.

2.4 SAP may document any discussions detailing or amending contractual provisions, especially the subject matter of the Order Form. Customer must check the discussion documentation as soon as possible and inform SAP of any necessary amendments or additions.

2.5 All works and goods provided by SAP to Customer before the conclusion of an Order Form (for example, proposals, test programs, designs) are property of SAP (see section 7). They must not be copied or made accessible to third parties. If no Order Form is concluded, they must be returned or deleted and must not be used. In all other respects the provisions of these present General Terms and Conditions, especially the exclusions and limitations of liability in section 10, apply to all contractual and precontractual obligations.

If, with Customer’s agreement, SAP provides Services other than those specified in the Order Form, the provisions and business terms of the Order Form are deemed also applicable to those Services.

2.6 Acceptance

2.6.1 SAP can require a written acceptance statement from Customer for all Contract Works within Services that are amenable to acceptance and may provide Customer with a template for such statement. Customer must accept Contract Works without delay subject to the provisions in this section 2.6. To this end an acceptance log can be created for signature by Customer.

2.6.2 If an Order Form specifies several Contract Works that Customer can use individually, those several Contract Works will be subject to separate acceptance.

2.6.3 If an Order Form specifies subsets of the Contract Works, SAP is entitled to submit subsets of the Contact Works for acceptance. Subsequent acceptance procedures will address only the correct functioning of the new subsets and whether the subsets accepted earlier correctly interact with the new subsets.

2.6.4 If the Order Form includes the creation of a design, for example for the implementation of standard software or the creation of modifications or add-ons to standard software, SAP can require that the design be subject to separate acceptance.

2.6.5 Customer must inspect the Contract Works within 15 working days and either notify SAP through the contact in writing that they are accepted or give a precise description of the defects found. If Customer does not give notice of acceptance or of defects within this period, or uses Contract Works without giving defect notice, the Contract Works will be deemed accepted. Immaterial defects are not grounds for withholding acceptance. In every case, Customer is deemed to have accepted any Contract Works it uses, in whole or any in part, in live operation.

2.6.6 SAP must remedy defects notified in accordance with section 2.6.5 within a period that is reasonable for the severity of the defect. Customer must inspect the Contract Works within five working days after notice that the defect has been eliminated. All other provisions in section 2.6.5 also apply with the necessary modifications.

3. CUSTOMER'S DUTY TO COLLABORATE

3.1 Customer must provide the operating environment (herein: "IT systems") necessary for the provision of Services, in accordance with SAP's guidance where given. It is the responsibility of Customer to secure proper operation of the IT systems by entering into maintenance contracts with third parties if necessary. In particular, Customer must follow SAP's instructions.

3.2 Free of charge, Customer must provide all collaboration that SAP requires in connection with performance of the Order Form, including, for example, human resources, IT systems, data, and telecommunications facilities. Customer must grant SAP direct and remote access to the software and the IT systems. Customer must answer questions and inspect results. Customer warrants that any materials provided by it for SAP to perform its contractual duties are free of defects in title that would preclude SAP from performing those duties.

3.3 Customer must nominate in writing a contact for SAP, with an address and email address at which the contact can be reached. The contact must be in a position to make necessary decisions for Customer or ensure that they are made without delay. Customer's contact must maintain effective cooperation with SAP's contact. Customer's employees whose activity is required must be freed from other activities to the appropriate extent.

3.4 Before commencing live operation with any provided Services, Customer must test it thoroughly for freedom from defects and for suitability in the situation. This also applies to Services it receives in connection with subsequent performance.

3.5 Customer must take appropriate precautions against the possibility that the Services may have or cause faults; such precautions include, for example, data backups, error diagnosis, and regular results monitoring. Except where otherwise expressly indicated in writing in individual cases, Consultants deployed by SAP are always entitled to act on the assumption that all data with which they come into contact is backed up.

3.6 Customer undertakes to provide all further collaborative goods, works, and services needed for the performance of the Order Form. If necessary, the Order Form will specify any other provisions.

3.7 Performance by Customer of its general collaborative duties is a primary contractual duty and necessary precondition for the correct performance by SAP of its Services.

3.8 Customer bears all consequences and costs resulting from breach of its duties and indemnifies SAP from all claims by third parties arising from such infringement.

4. CHANGE REQUEST PROCEDURE

4.1 During the term of a project, both parties can request changes through their respective contacts (see section 3.3), in writing, to the agreed Services, methods, dates and times, and other details.

4.2 If Customer makes a change request, SAP must inform Customer within 10 working days whether the change is possible or not and what impact the change would have on the Order Form with particular reference to the timeline and remuneration. Customer must thereupon inform SAP in writing within 5 working days whether the change request is to apply or whether the Order Form is to be continued on the existing terms. If the investigation of a change request itself requires substantial work, SAP is entitled to bill separately for that work.

4.3 If SAP submits a change request, Customer must notify SAP in writing within 10 working days whether it accepts the change or not.

4.4 Until there is agreement about the change, work will continue in accordance with the existing Order Form. Alternatively, Customer can require that all or part of the work be suspended or permanently ended in accordance with and subject to section 12.1.

With effect from the first working day of suspension, remuneration is payable at the agreed rate, or, in default of an agreed rate, at the daily rate in the Services PCL, in respect of each SAP employee whose work is suspended and each day of the suspension. The legal consequences of final cancelation are as provided in the German Civil Code, section 648a.

5. FEES; PAYMENT; TAXES; RETENTION OF RIGHTS

5.1 Fees

5.1.1 Unless otherwise agreed in writing, the remuneration payable will be determined by the Services PCL valid from time to time.

5.1.2 SAP is entitled to submit invoices for subsets of the Services.

5.1.3 Any resource-related invoice must include a list of the activities to which it refers. The listed details are deemed accepted unless Customer rejects them in writing within two weeks.

5.1.5 SAP is entitled to require full or part payment in advance if there is no prior business relationship with Customer, if delivery is to be made outside Germany, if Customer's registered office is outside Germany, or if there are any grounds to doubt that Customer will render payment punctually.

5.1.6 Customer is entitled to offset only claims that are uncontested or ordered by a court of law and to withhold payment or retain possession only to secure claims that are uncontested or ordered by a court of law. Subject to the provisions of the German Commercial Code, section 354a, it cannot assign its claims to a third party.

5.1.7 SAP retains all title to and rights (section 7) in the Services until full satisfaction of its claims under the Order Form. Customer must immediately notify SAP in writing if any third party gains access to the property to or in which SAP retains title or rights and must also inform the third party of SAP's rights.

5.2 Invoicing; Due date. Payments are due 14 days after invoicing. No cash discount is available. SAP is entitled to charge late-payment interest from the due date at the statutory rate of penal interest.

5.3 Taxes. All prices are subject to statutory sales tax / VAT.

6. TERM / TERMINATION

6.1 Term of Order Form. Unless otherwise agreed in the relevant Order Form, every Order Form comes into force on the date it was last signed and runs for the term specified in the Order Form.

6.2. Termination. Unless otherwise agreed, an Order Form may not be terminated with due notice. Extraordinary termination rights and the right to termination for just cause remain unaffected.

Just cause for termination includes, without limitation, when Customer fails to perform a major contractual obligation within 30 days of written warning from SAP, notably, for example, when the Customer is more than 30 days in default of a payment due and payable under the Order Form.

6.3 Effect of Termination. Upon termination of the Order Form, the parties shall irretrievably return all Confidential Information to the party that disclosed it, or at the disclosing party's request, destroy the Confidential Information of disclosing party and certify that it has complied with these obligations.

7. RIGHTS

Between Customer and SAP all title to and rights in the Services vest in SAP and (its parent company) SAP SE, exclusively, notably copyright and rights of authorship, rights to inventions, and other industrial property rights, and including without limitation Services created to address the requirements of or in cooperation with Customer. Except as otherwise agreed in writing, once the installments due up to and including the acceptance have been paid in full, Customer is granted a non-exclusive license to the same extent and for same time-period, as granted to him by SAP under the corresponding Software Agreement.

Before accepting them, Customer may use the Services only to the extent necessary for test purposes. Customer is permitted to create necessary backup copies of the Services. Backup copies must be marked as backup copies and bear the same copyright and authorship notice as the original.

8. CONFIDENTIALITY; DATA PROTECTION

8.1 Use of Confidential Information. Each party undertakes forever to treat as confidential all Confidential Information of the other acquired in connection with the performance or processing of the Order Form and to use such information and secrets only to perform the Order Form. Confidential Information shall not be reproduced in any form except as required to accomplish the intent of the respective Order Form or processing the Order Form. Any reproduction of any Confidential Information of the other party shall remain the property of the other party and shall contain any and all confidential or proprietary notices or legends which appear on the original.

With respect to the Confidential Information of the other party, each party: (a) shall take all reasonable steps (defined below) to keep all Confidential Information strictly confidential; (b) shall not disclose or reveal any Confidential Information to any person other than its representatives who need to know this Information to fulfill that party's contractual obligations or to processing the Order Form. As used herein, “reasonable steps” means those steps the receiving party takes to protect its own similar Confidential Information, which shall not be less than a reasonable standard of care; this includes Customer's careful safekeeping and protection of Confidential Information against misuse.

8.2 Exceptions. The above section 8.1 does not apply to any Confidential Information that: (a) is independently developed by the receiving party without recourse to the Confidential Information of the disclosing party, or is received lawfully and free of duty of confidentiality from a third party having the right to furnish such Confidential Information; (b) has become generally available to the public without breach of the Order Form by the receiving party; (c) at the time of disclosure to the receiving party was known to be free of restrictions; or (d) the disclosing party agrees in writing is exempt from the above provisions; or (e) is rightfully acquired by the receiving party from a third party who has the right to disclose it and who provides it without restriction as to use or disclosure.

8.3 Confidential Terms and Conditions; Publicity. Customer shall treat as confidential the terms and conditions of the respective Order Form, in particular the pricing contained therein. Neither party shall use the name of the other party in publicity, advertising, or similar activity, without the prior written consent of the other. However SAP may use Customer's name in customer listings (reference listings) or to analyze details from the Order Form (for example, to forecast demand), as well as – subject to mutual agreement – as part of SAP's other marketing efforts. This includes the provision for forecast analysis to and use by SAP Affiliates. Insofar as this includes the provision and use of contact information of Customer’s contact persons, Customer shall secure the appropriate permissions where necessary.

8.4 Data Protection. The final provisions on data protection obligations of the contract partners in the context of possible order data processing (in particular in the context of troubleshooting or the elimination of defects in the context of the Order Form) result from the Annex “Personal Data Processing Agreement for SAP Support and Professional Services” attached to these Services GTC.

9. DEFECTS AS TO QUALITY AND DEFECTS IN TITLE, OTHER FAULTS

9.1 In respect of any Contract Work that falls within the ambit of the statutory liability for quality and title defects, SAP warrants, subject to sections 9.1 to 9.7, that the Contract Work has the expressly agreed qualities and that no third-party rights are infringed by the grant of rights to Customer in section 7. Where no qualities have been agreed, SAP warrants that the Contract Work is suitable for the use envisioned in the Order Form or, in the absence of an envisioned use, for ordinary use, and that it has the qualities that are usual and that a customer can expect from Contract Works of its kind.

9.2 Customer must notify SAP in writing without delay if it identifies defects and must include a precise description of the problem and the information that is useful for eliminating the defect. So far as is reasonable in ordinary business, Customer must inspect the Contract Works without delay after SAP delivers them and, if a defect is apparent, notify SAP of it without delay. If Customer does not notify SAP of the defect, the Contract Works are deemed to be approved, unless the defect was not apparent at the time of inspection. If such a defect subsequently becomes apparent, Customer must notify SAP without delay after discovering the defect; otherwise, the Contract Works are deemed to be approved despite the presence of the defect. Customer’s rights are secured if the notification was received in time. SAP cannot rely on the provisions in sentences 2 to 5 in this section if SAP has fraudulently concealed the defect. Notice of a defect as described above is effective only if given by the contact (see section 3.3).

9.3 Where defects as to quality are duely notified, SAP will discharge its warranty by remedying the defect either by providing Customer with a new version of the Contract Works that is free of defects or, at SAP’s discretion, by eliminating the defect. One of the ways SAP may eliminate a defect is to indicate to Customer a reasonable way to avoid the effect of the defect. To discharge its liability for defects in title, SAP will remedy shown defects either by procuring for Customer the legally incontestable right under license to use the delivered Contract Works or, at SAP’s election, providing equivalent replacement or altered Contract Works. Customer must accept a new version of the Contract Works that is functionally compliant unless it would be unreasonable to require Customer to do so. The level of urgency of error-correction work will reflect the extent to which business operations are impeded. These present provisions, in particular section 3, also apply as appropriate.

9.4 If Customer sets a reasonable limited additional time period for SAP to remedy the defect and SAP finally fails to do so in that time, Customer has the right to rescind the Order Form or terminate continuing or recurring contractual obligations or reduce the remuneration. The requirements in section 12.1 must be met with regard to fixing a reasonable limited additional time period. Subject to the exclusions and limitations in section 10, SAP undertakes to compensate for loss or wasted anticipatory expenditure caused by a defect. Other remedies for defects as to quality or defects in title are excluded.

9.5 The time bar for claims under sections 9.1 to 9.4 comes into effect one year after delivery of the Contract Works in accordance with section 2.6 This also applies to rights arising out of rescission or reduction of remuneration under section 9.4, sentence 1. The reduction in the time before the time bar comes into effect does not apply in cases of SAP’s intent or gross negligence, of fraudulent concealment of a defect, of personal injury, or of defect in title to which the German Civil Code, section 438 (1)(1)(a) applies.

9.6 Where works or services are delivered to eliminate or avoid a defect, the time bar for claims for defects in those works and services comes into effect at the time specified in section 9.5. However, the time before the bar comes into effect is suspended while, with Customer’s consent, SAP is checking the existence of a defect or is remedying a defect, until SAP informs Customer of the results of its check, gives notice that the remedy is complete, or refuses to remedy the defect. The time bar comes into effect three months after the end of the toll.

9.7 If SAP provides defect identification or elimination works or services without being under obligation to do so, SAP is entitled to remuneration under section 5.1. This applies in particular to any reported quality defect that is not reproducible or not imputable to SAP or in cases where the SAP Software or Contract Works is not used in compliance with its documentation. Without prejudice to the generality of the foregoing, SAP is entitled to remuneration for additional works or services it does to eliminate any defect that arises out of Customer’s failure to properly discharge its duty to collaborate, inappropriate operation of the SAP Software, or failure to take the SAP services that SAP recommends.

9.8 If a third party claims that the exercise of the license granted under the Order Form infringes its rights, Customer must fully inform SAP in writing without delay. If to mitigate loss or for other good reason Customer ceases to use the Services, Customer must notify the third party that such cessation does not imply any recognition of the claimed infringement. Customer will conduct the dispute with the third party in court only in consultation and agreement with SAP or authorize SAP to assume sole conduct of the dispute.

9.9 If SAP fails to properly perform any of its duties herein that is not within the ambit of defect liability, or is otherwise in breach, Customer must give notice of the failure or breach to SAP in writing and fix a limited additional time period during which SAP has the opportunity to properly perform its duty or otherwise rectify the situation. Section 12.1 applies. SAP will compensate for loss or wasted anticipatory expenditure subject to the exclusions and limitations in section 10.

10. LIABILITY

10.1 SAP is liable in contract, tort, or otherwise for loss or wasted expenditure subject always as follows:

10.1.1 In cases of intent, SAP's liability extends to the full loss; in cases of gross negligence, SAP's liability is limited to the amount of foreseeable loss that would have been prevented through the exercise of due care; in cases of absence of a guaranteed quality, SAP's liability is limited to the amount of foreseeable loss that would have been prevented by the presence of the guaranteed quality.

10.1.2 In other cases: SAP is not liable except for breach of a major obligation (Kardinalpflicht)

This is a translation. The agreed General Terms and Conditions are those in the original German document and only up to the limits in the following subsection. A breach of a major obligation in the meaning of section 10.1.2 is assumed where the duty itself is a necessary prerequisite for the contractual performance, or where the breach of the relevant duty jeopardizes the purpose of the contract and where Customer could legitimately rely upon its fulfillment.

Liability in cases under section 10.1.2 is limited to €200,000 per incident and limited in total to €500,000 for all claims arising out of the Order Form .

10.2 Contributory fault and contributory negligence may be claimed. The limits of liability in section 10.1 do not apply to liability for personal injury, or to liability under the German Product Liability Act (Produkthaftungsgesetz).

10.3 All claims against SAP in contract, in tort, or otherwise for loss or wasted anticipatory expenditure are barred after a period of one year. That period begins at the point in time specified in the German Civil Code (BGB), section 199 (1). The time bar comes into effect not later than five years after the claim arises. The provisions in sentences 1 to 3 in this section do not apply to liability for intent or gross negligence, liability for personal injury, or liability under the German Product Liability Act. The provisions in this section do not affect the other time bar for claims arising out of defects as to quality and defects in title (sections 9.5 and 9.6).

11. CONTRACT TRANSFER

Customer is not entitled to transfer the

Order Form or any rights or obligations thereunder to any third party.

12. MISCELLANEOUS PROVISIONS

12.1 Contractual collaboration requires a high level of trust, interaction, and willingness to agree. Except in emergencies, a limited time fixed by Customer pursuant to the law or contract must not be less than 10 working days. Failure to comply with any fixed time limit entitles Customer to be released from the Order Form (for example, by rescission, termination, or claim for damages in lieu of performance) or to a price reduction for breach only if this was threatened in writing in the notice fixing the limited time as a consequence of failure to comply with that time limit. After a limited time fixed in accordance with sentence 2 expires, SAP is entitled to give notice to Customer requiring that any rights arising out of the expiration be exercised within two weeks of receipt of the notice.

12.2 SAP has four weeks to accept offers made by Customer. Offers from SAP are nonbinding unless otherwise agreed in writing. In cases of conflict, the Order Form terms and details that apply are those in SAP's offer or confirmation.

12.3. Period During Which Services Will Be Provided

12.3.1 Dates and times are nonbinding except where Customer and SAP have expressly agreed in writing that they are binding. SAP's duty to realize a design or concept does not commence until Customer accepts the design or concept.

12.3.2 If SAP has to wait for collaboration or information from Customer or is otherwise hindered in the performance of the Order Form by any strike, lockout, official intervention, or any other circumstance where it is not at fault, times for delivery of goods and provision of Services are extended by a period equaling the duration of the hindrance plus a reasonable start-up period after the end of the hindrance. SAP must notify Customer of the hindrance.

12.3.3 Working days are weekdays from Monday to Friday (8 a.m. to 5 p.m. CET) except German national public holidays and December 24 and 31.

12.4 The Services, including the associated SAP Software, are subject to the export control laws of various countries, including without limit the laws of the United States and Germany. Customer agrees that it will not submit the Services to any government agency for licensing consideration or other regulatory approval without the prior written consent of SAP, and will not export the Services to countries, persons or entities prohibited by such laws. Customer shall also be responsible for complying with all applicable legal regulations of the country where Customer is registered, and any foreign countries with respect to the use of the SAP Software by Customer and its Affiliates.

12.5 German law applies exclusively to all claims in contract, in tort or otherwise, and the UN sales laws convention is excluded. Conflict-of-law rules do not apply. If Customer is a merchant within the meaning of the German Commercial Code (HGB), section 1, or a public-law juristic person or special fund, the sole place of jurisdiction for all differences arising out of or in connection with this Services GTC and/or any related Order Form shall be Karlsruhe.

12.6 Amendments or additions and contractually relevant declarations as well as declarations directly influencing a legal relationship, especially without being limited to termination notices, reminders or notices to set time limits, require written form. The foregoing provision also applies to any waiver of the written-form requirement. The written-form requirement can also be met by exchange of letters or (except in the case of termination notices) with an electronically transmitted signature (facsimile transmission, e-mail transmission with scanned signatures, or other agreed form of contract conclusion provided by or on behalf of SAP, such as SAP Store). Except in that respect, however, the provisions in the German Civil Code (BGB), sections 127 (2) and (3) do not apply.

12.7 A separate agreement is required for any other goods, works and services that are not expressly described in the respective Order Form . Unless otherwise agreed, such goods, works and services are provided subject to SAP's General Terms and Conditions for SAP Services and SAP is entitled to remuneration for them in accordance with the relevant SAP list of prices and conditions.

ANNEX "PERSONAL DATA PROCESSING AGREEMENT FOR SAP SUPPORT AND PROFESSIONAL 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 provided by Customer and each Data Controller in connection with the performance of the SAP services as set out in the relevant Agreement ("SAP Service(s)") to which is attached the present DPA which may include:

(a) SAP Support as defined in the Software License & Support Agreement; and/or

(b) Professional Services as described in the services agreement concluded between SAP and the Customer ("Services Agreement").

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, the categories of data, the 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 include Personal Data in systems accessible by SAP when performing the SAP 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. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to include Personal Data 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 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.

Appendix 2 applies only to the extent that such SAP Services are performed on or from SAP premises. In the case where SAP is performing SAP Services on the Customer's premises and SAP is given access to Customer's systems and data, SAP shall comply with Customer's reasonable administrative, technical, and physical conditions to protect such data and guard against unauthorized access. In connection with any access to Customer's system and data, Customer shall be responsible for providing SAP personnel with user authorizations and passwords to access its systems and revoking such authorizations and terminating such access, as Customer deems appropriate from time to time. Customer shall not grant SAP access to Licensee systems or personal information (of Customer or any third party) unless such access is essential for the performance of SAP Services. Customer shall not store any Personal Data in non-production environments.

2.2 Changes. SAP applies the technical and organizational measures set forth in Appendix 2 to SAP's entire customer base receiving the same SAP 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 Customer may provide further instructions during the performance of the SAP Service. 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 performance of the SAP 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 will correct or remove any Personal Data in SAP´s possession (if any), 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 SAP Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

4. DATA DELETION

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 six months) once Personal Data is no longer required for execution of the Agreement, 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 service and support delivery centers and IT 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 through providing a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate). Certifications are available under: https://www.sap.com/corporate/en/company/quality.html#certificates or upon request if the certification is not available online; or

(b) A Personal Data Breach has occurred; or

(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, time frame and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited to remote audits where possible. If an on-site audit is mandatory, it shall not exceed one business day. 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 the 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;

(c) For SAP Support SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP (under: https://support.sap.com/en/my-support/subprocessors.html) or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the SAP Service; and

(d) For Professional Services, SAP will, upon request of the Customer, make the list available or identify such subprocessors prior to the start of the applicable SAP Services.

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

(a) SAP will inform Customer in advance of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor (i) for SAP Support - by posting on the SAP Support Portal, or by email, upon Customer's registration on the SAP Portal and (ii) for Professional Services – by similar posting on the SAP Support Portal, or by e-mail, or in other written form;

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

6.3 Objections to New Subprocessors.

(a) SAP Support: If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the SAP Support upon written notice to SAP, such notice to be provided to SAP no later than thirty days from the date SAP informs the Customer of the new Subprocessor. If Customer does not provide SAP with a notice of termination within this thirty days period, Customer is deemed to have accepted the new Subprocessor. Within the thirty days period from the date of SAP informing the 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 providing SAP a notice of termination and does not affect SAP's right to use the new Subprocessor(s) after the thirty days period.

(b) Professional Services: If Customer has a legitimate reason under Data Protection Law that relates to the Subprocessors' processing of Personal Data, Customer may object to SAP's use of a Subprocessor, by notifying SAP in writing within five business days of SAP's information as per Section 6.2. If Customer objects to the use of the Subprocessor, the parties will come together in good faith to discuss a resolution. SAP may choose to: (i) not use the Subprocessor or (ii) take the corrective steps requested by Customer in its objection and use the Subprocessor. If none of these options are reasonably possible and Customer continues to object for a legitimate reason, either party may terminate the relevant services on five days' written notice. If Customer does not object within five days of receipt of the notice, Customer is deemed to have accepted the Subprocessor. If Customer's objection remains unresolved thirty days after it was raised, and SAP has not received any notice of termination, Customer is deemed to have accepted the Subprocessor.

(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 (d), or a notice to Customer; and/or

(c) Other Controllers who have been authorized by Customer to include Personal Data 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. DEFINITIONS

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

9.1 "**Authorized Users**" means any individual to whom Customer grants access authorization in compliance with a SAP software license to use the SAP Service that is an employee, agent, contractor or representative of (i) the Customer, (ii) Customer's Affiliates, and/or (iii) Customer's and Customer's Affiliates' Business Partners (as defined under the Software License and Support Agreement).

9.2 **"Controller"** means the natural or legal person, public authority, agency or other body, which alone or jointly with others, determines the purposes and means of 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.

9.3 **"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).

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

9.5 **"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 supplied to or accessed by SAP or its Subprocessors in order to provide the SAP Service under the Agreement.

9.6 **"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.

9.7 **“Professional Services”** means implementation services, consulting services and/or services such as SAP Premium Engagement Support Services, Innovative Business Solutions Development Services, Innovative Business Solutions Development Support Services.

9.8 **“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.

9.9 **“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). The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Appendix 4.

9.10 **“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 SAP Service and which processes 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 concluded a Software License and Support Agreement and/or Services Agreement with SAP under which it benefits from SAP Service as described under the relevant Agreement. The Data Exporter allows other Controllers to also use the SAP Service, these other Controllers are also Data Exporters.

Data Importer

SAP and its Subprocessors provide the SAP Service as defined under the relevant Agreement concluded by the Data Exporter that includes the following SAP Service:

- Under the Software License and Support Agreement: SAP and/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 handles support tickets in a tracking system
- under the applicable Services Agreement for Professional Services: SAP and/or its Subprocessors provide Services subject to the Order Form Services and the applicable Scope Document.

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 transmitted to, made available or accessed by the Data Importer.

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. 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 transferred by Authorized Users and may include financial data such as 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 basic processing activities as set out in the Agreement which may include:

- use of Personal Data to provide the SAP Service
- storage of Personal Data
- computer processing of Personal Data for data transmission
- execution of instructions of Customer in accordance with the Agreement.

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

1. TECHNICAL AND ORGANIZATIONAL MEASURES

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

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

Measures:

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

Additional measures for Data Centers:

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

1.2 System Access Control. Data processing systems used to provide the SAP 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 to 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 SAP Services in accordance with the relevant 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 required for data transfer are hereby mutually agreed upon between SAP and its customer and included as a part of the 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 SAP Service to the extent technically possible.

1.6 Job Control. Job Control is required to ensure that personal data processed on behalf of others are processed strictly in compliance with the Customer's instructions

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.

  For Support Services, SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer system without the knowledge and consent of the customer. For Support Services, SAP provides a specially designated, secure support ticket facility in which SAP provides a special access-controlled and monitored security area for transferring access data and passwords. SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer on premise system without the knowledge and active participation of the customer.

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 continuity plans for business-critical processes;
- 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 appropriate technical controls to achieve Customer Data separation at all times.
- Customer (including its approved Controllers) will have access only to their own Data based on secure authentication and authorization.
- 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. In particular:

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

Appendix 3 to the DPA

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	1.1and Appendix 1, 1.2	Purpose and Aplication, Appendix 1 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 Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) (c)	7.2 and Appendix 4	Standard Contractual Clauses. and Appendix 4 Standard Contractual Clauses (Processors)

Appendix 4 to the DPA
Standard Contractual Clauses (Processors)[*]

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

[…]
(in the Clauses hereinafter referred to as the '**data exporter'**)

and

[…]
(in the Clauses hereinafter referred to as the **'data importer'**)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1];

(b) 'the data exporter' means the controller who transfers the personal data;

(c)'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7,Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in

[*] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c)that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer [2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii)any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing law

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

Clause 10

Variation of the contract

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

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses ([3]). Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.