DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

1. PREAMBLE

1.1 Schedule.

This document including Attachment 1, Appendices 1 and 2 ("**Schedule**") shall become an integral part of the Agreement through its reference from the Order Form signed by Customer. This Schedule serves as a written data processing agreement between SAP and, subject to Section 1.2 below, each Data Controller providing Personal Data in connection with its use of the Cloud Service. It furthermore defines the applicable technical and organizational measures SAP implements and maintains to protect Personal Data stored in the production system of the Cloud Service.

1.2 Direct Contractual Relationship.

(a) If the processing of Personal Data by SAP is conducted within the EEA, this Schedule applies between SAP and Customer. In this case, Customer is responsible to flow down the terms and conditions set out in this Schedule to its Affiliates.

(b) If Customer and/or its Affiliates are located within the EEA and SAP or its Subprocessors are processing or accessing Personal Data outside the EEA Sections 5.1 and 5.2 of this Schedule apply.

1.3 Form.

The conclusion of the Agreement which incorporates this Schedule shall be evidenced upon SAP's receipt of any of the following:

(a) signed original Order Form,

(b) signed Order Form in pdf or similar format, or

(c) accepted Order Form using DocuSign or a similar product used by SAP to receive an Order Form from Customer.

Should Customer require a written original copy of this Schedule or a separately signed electronic copy of the Schedule it shall submit a request to its SAP sales representative.

1.4 Governance.

Customer acts as the Data Controller concerning Personal Data of its own Authorized Users as well as on behalf of and in the name of its Affiliates or third parties in their capacity as Data Controllers permitted by Customer to use the Cloud Service. Customer shall serve as a single point of contact for SAP and is solely responsible for the internal coordination, review and submission of instructions or requests of other Data Controllers to SAP. SAP shall be discharged of its obligation to inform or notify a Data Controller when it has provided such information or notice to Customer. SAP is entitled to refuse any requests or instructions provided directly by a Data Controller that is not the Customer. Customer warrants that it is entitled to disclose Personal Data to SAP within the Cloud Service as per the Agreement. Customer agrees to hold SAP harmless for claims brought against SAP or its Subprocessors in connection with any breaches of the Customer's Data Protection duties.

1.5 Severability.

If any provision of this Schedule is found by any court of competent jurisdiction to be invalid or unenforceable, the invalidity of such provision shall not affect the other provisions of this Schedule, and all provisions not affected by such invalidity shall remain in full force and effect.

2. DATA PROCESSING PURPOSES

2.1 Appendix 1.

Customer and the respective Data Controllers shall determine the purposes of collecting, processing, and otherwise using Personal Data stored in the Cloud Service. Unless provided otherwise in the Agreement, Appendix 1 of the Schedule shall apply to such data processing.

2.2 Purposes.

The purposes for processing Personal Data by SAP and its Subprocessors under this Schedule are limited to:

(a) Setting up, operating, monitoring and providing the Cloud Service, including the underlying infrastructure (hardware, software, secure data center facilities, connectivity), as a Data Processor or Subprocessor as set forth in the Agreement,

(b) Providing technical support as a main obligation of SAP under the Agreement,

(c) Providing Consulting Services as a main obligation of SAP, if and to the extent agreed by the parties,

(d) Communicating to Authorized Users as clarified in the terms associated with a particular Cloud Service and

(e) Executing instructions of Customer in accordance with Sections 3.1 and 3.2 below.

3. SAP OBLIGATIONS

3.1 Instructions.

SAP shall process Personal Data only in accordance with each Data Controller's instructions submitted by Customer. SAP shall use reasonable commercial efforts to follow and comply with the instructions received from Customer as long as they are legally required and technically feasible and do not require any material modifications to the functionality of the Cloud Service or underlying software. SAP shall notify Customer if SAP considers an instruction submitted by Customer to be in violation of the applicable Data Protection Law. SAP shall not be obligated to perform a comprehensive legal examination. If and to the extent SAP is unable to comply with an instruction it shall promptly notify (email permitted) Customer hereof.

3.2 Instructions based on Data Subject Remedies.

SAP may, upon the instruction of Customer and with Customer's necessary cooperation, correct, erase and/or block any Personal Data if and to the extent the functionality of the Cloud Service does not allow Customer, its Data Controllers or Authorized Users to do so. In the event that SAP needs to access any of Customer's systems or Customer's instance of the Cloud Service remotely to execute an instruction or provide technical support, e.g. via application sharing, Customer hereby grants to SAP the permission for such remote access. Further, Customer will name a contact person that – if necessary – can grant to SAP the required access rights.

3.3 Data Secrecy.

For processing Personal Data, SAP and its Subprocessors shall only use personnel who are subject to a binding obligation to observe data secrecy or secrecy of telecommunications, to the extent applicable, pursuant to the Data Protection Law. SAP shall itself and shall require that its Subprocessors regularly train individuals to whom they grant access to Personal Data in data security and data privacy.

3.4 Technical and Organizational Measures.

(a) SAP shall, as a minimum, implement and maintain appropriate technical and organizational measures as described in Appendix 2 of the Schedule.

(b) Appendix 2 applies to the production system of the Cloud Service to keep Personal Data secure and protect it against unauthorized or unlawful processing and accidental loss, destruction or damage. Non-production environments (e.g. a test instance of the Cloud Service) provide for a lower level of security and SAP recommends that Customer does not store any Personal Data in such non-production environments.

(c) Since SAP provides the Cloud Service to all customers uniformly via a hosted, web-based application, all appropriate and then current technical and organizational measures apply to SAP's entire customer base hosted out of the same data center and subscribed to the same Cloud Service. Customer understands and agrees that the technical and organizational measures are subject to technical progress, development and improvements for the protection of Personal Data shall automatically apply.

3.5 Verification.

SAP shall regularly test the measures described in Appendix 2. If a Data Controller believes that additional measures are required under the applicable Data Protection Law Customer shall submit an instruction according to Section 3.1 above.

3.6 Security Breach Notification.

SAP shall promptly inform Customer as soon as it becomes aware of serious disruptions of the processing operations, or any Security Breach in connection with the processing of Personal Data which, in each case, may significantly harm the interest of the Data Subjects concerned.

3.7 Cooperation.

At Customer's request and expense, SAP shall reasonably support Customer or other Data Controllers in dealing with requests from individual Data Subjects and/or a supervisory authority with respect to the processing of Personal Data hereunder.

3.8 Deletion.

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

4. SUBPROCESSORS

4.1 Permitted Use.

(a) Customer (also on behalf of its Data Controllers) hereby authorizes SAP (also for the purpose of Clause 11 paragraph 1 of the Standard Contractual Clauses) to engage subcontractors for the processing of Personal Data (each a **"Subprocessor"**) (i) to the extent necessary to fulfill its contractual obligations under the Agreement and (ii) as long as SAP remains responsible for any acts or omissions of its Subprocessors in the same manner as for its own acts and omissions hereunder.

(b) SAP shall pass on to Subprocessors SAP's obligation as Data Processor (or Subprocessor) vis-à-vis Customer and the respective Data Controllers as set out in this Schedule.

(c) SAP undertakes to have a selection process by which it evaluates the security, privacy and confidentiality practices of a Subprocessor in regards to data handling on a scheduled basis. Alternatively, the Subprocessor shall possess a security certification that evidences appropriate security measures are in place with regard to the Subprocessor's services to be provided to SAP.

(d) SAP will inform Customer upon its request by email about the name, address and role of each Subprocessor it uses to provide the Cloud Service.

4.2 New Subprocessors.

(a) SAP may remove, replace or appoint suitable and reliable further Subprocessors at its own discretion in accordance with this Section 4.2.

(b) SAP will notify Customer by email in advance (except for Emergency Replacements under Section 4.3) of any changes to the list of Subprocessors. If Customer does not object in accordance with Section 4.2 (c) within thirty days after receipt of SAP's notice the new Subprocessor(s) shall be deemed accepted.

(c) If Customer has a legitimate reason to object to SAP's use of a Subprocessor (e.g. if the Subprocessor is a Non-EEA Entity and Customer needs to complete additional formalities as a Data Controller prior to the use of such Subprocessor) Customer shall notify SAP thereof in writing within thirty days after receipt of SAP's notice. If Customer objects to the use of the Subprocessor concerned SAP shall have the right to cure the objection through one of the following options (to be selected at SAP's sole discretion): (i) SAP will abort its plans to use the Subprocessor with regard to Personal Data; or (ii) SAP will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the Subprocessor with regard to Personal Data; or (iii) SAP may cease to provide or

Customer may agree not to use (temporarily or permanently) the particular aspect of the Cloud Service that would involve use of the Subprocessor with regard to Personal Data. If none of the above options are reasonably available and the objection has not been cured within thirty days after SAP's receipt of Customer's objection, either party may terminate the affected Cloud Service with reasonable prior written notice.

4.3 **"Emergency Replacement"** refers to a sudden replacement of a Subprocessor where such change is outside of SAP's reasonable control (such as if the Subprocessor ceases business, abruptly discontinues services to SAP, or breaches its contractual duties owed to SAP). In such case, SAP will inform Customer of the replacement Subprocessor as soon as possible and trigger the process to formally appoint such Subprocessor pursuant to Section 4.2.

5. INTERNATIONAL TRANSFERS AND COUNTRY-SPECIFIC DEVIATIONS

5.1 International Transfer.

Personal Data that SAP has received from any Data Controller located in the EEA shall only be exported by SAP or its Subprocessors from the Data Center (whether located in or outside the EEA) to or accessed from a country or territory outside the EEA (**"International Transfer"**) if

(a) the recipient itself or the country or territory in which it operates (i.e. where or from where it processes or accesses Personal Data) has been found to ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data as determined by the European Commission and subject to the scope restrictions of any such determination; or

(b) the International Transfer to a Non-EEA Entity is in accordance with Section 5.2 below.

5.2 Standard Contractual Clauses. Multi-tier Framework.

(a) The Standard Contractual Clauses attached to this Schedule (**"Attachment 1"**) and Section 4 above apply if the Agreement is concluded between (i) an EEA based Customer or (ii) a Customer with EU based Customer Affiliates and an SAP entity located outside the EEA.

(b) For any other International Transfer where SAP uses further Non-EEA Entities (appointed under Section 4 above), SAP (represented by SAP SE) has entered into the unchanged version of the Standard Contractual Clauses with each Non-EEA Entity prior to processing Personal Data by means of an International Transfer.

(c) Customer hereby accedes, and each Data Controller may accede, to the Standard Contractual Clauses set forth in paragraph (b).

(d) If the preceding direct contract is not available to a Data Controller under mandatory Data Protection Law as determined by SAP and Customer, the Data Controller may enter into the Standard Contractual Clauses furnished by SAP with the relevant Non-EEA Entity (represented by SAP SE).

(e) In the event such direct right to enforce the Standard Contractual Clauses against the relevant Non-EEA Entity does not exist for the Data Controller or is successfully challenged by a Subprocessor, SAP shall enforce such Standard Contractual Clauses against the Subprocessor on behalf of the Data Controller in compliance with this Schedule.

(f) Nothing in the Agreement shall be construed to prevail over any conflicting Clause of the Standard Contractual Clauses.

(g) The Standard Contractual Clauses shall be governed by the law of the Member State in which the EU based Data Exporter is established.

5.3 Country-specific Deviations.

(a) **Australia.** (i) For the purposes of this Schedule - "**APP**' means the Australian Privacy Principles, from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, and which amended the Privacy Act 1988; **"Data Controller"** means a person who, alone or jointly or in common with other persons, determines the purposes and manner in which any Personal Data are, or are to be, processed; and **"Data Processor"** shall mean any person (other than an employee of the Data Controller) who processes Personal Data on behalf of the Data Controller. (ii) To the extent a Data Controller in Australia or its Authorized Users intend to enter Personal Data into the Cloud Service, Customer agrees to first obtain the consent of each Data Subject to an International Transfer as contemplated under this Schedule if and to the extent required under the applicable data protection law in Australia. Customer hereby confirms and commits that it has received the Personal Data and informed the related Data Subjects regarding the disclosure of the Personal Data in accordance with the APP, and Privacy Act 1988. As such, and on that basis, APP 8.1 is satisfied and shall not otherwise apply by virtue of the "informed consent" exception under APP 8.2(b) (**"Informed Consent"**). To the extent that Informed Consent may not apply, this Schedule provides the framework for the protection of that Personal Data of those Australian Data Subjects in a way that, overall, is at least substantially similar which the APP's protect that information and SAP agrees to afford to such Personal Data a similar level of protection as set forth in Sections 2, 3 and 6 of this Schedule (by virtue of the "substantially similar law" exception under APP 8.2(a)) (**"Substantially Similar Law"**), and as such, and on that basis, APP 8.1 is satisfied and shall not otherwise apply by virtue of Substantially Similar Law.

(b) **Austria**. To the extent a Data Controller in Austria or its Authorized Users intend to enter personal data of legal entities (also considered personal data under the Federal Act concerning the Protection of Personal Data (DSG 2000)) into the Cloud Service, Customer agrees to first obtain the consent (in the sense of § 12 para. 3 of the DSG 2000) of such legal entity (Data Subject) before using the Cloud Service, as described herein, for such Data Subject(s). SAP agrees to afford to such personal data a similar level of protection as set forth in Sections 2, 3 and 6 of this Schedule.

(c) **Russian Federation**. Customer or Customer Affiliates as Data Controllers remain operators of Personal Data of Russian citizens submitted for processing to SAP and are responsible for determining (i) if Customer will be able to comply with applicable Russian privacy law in use of the Cloud Service which involve processing of Russian citizen's Personal Data and (ii) whether the Cloud Service can be used inside or outside the Russian Federation.

(d) **Singapore.** In accordance with regulation 10(2)(b) of the Personal Data Protection Regulations 2014, unless otherwise stated in the Order Form, the countries to which SAP may transfer Personal Data contained in the Customer Data in the provision of the Cloud Service under the Agreement (as of the effective date of the Order Form signed by Customer) are Australia, Austria, Brazil, Bulgaria, Canada, Chile, China, China/Hong Kong, Czech Republic, France, Germany, Hungary, India, Ireland, Israel, Malaysia, Mexico, the Netherlands, Peru, the Philippines, Poland, the Russian Federation, Singapore, Slovakia, South Africa, South Korea, Spain, Sweden, the United Kingdom, and the United States of America. SAP may add new countries to the above list of countries via the process for notifying Customer of any changes to SAP's list of Subprocessors set forth in Section (d) above, with such notice to include the country in which any new Subprocessor is located. This Section does not necessarily include all countries to which SAP may transfer Customer Data at the direction of Customer or the countries from which Customer, its Authorized Users or Customer's Business Partners may access the Cloud Service.

(e) **South Korea.** To the extent a Data Controller in Republic of Korea or its Authorized Users intend to enter Personal Data into the Cloud Service, Customer agrees to first obtain the consent of each Data Subject to an International Transfer as contemplated under this Schedule if and to the extent required under the applicable Personal Information Protection Act in Republic of Korea. Customer hereby confirms and commits that it has received the Personal Data and informed the related persons regarding the transfer/process of the Personal Data in accordance with the applicable law.

(f) **Switzerland.** To the extent a Data Controller in Switzerland or its Authorized Users intend to enter personal data of legal entities (also considered personal data under the Swiss Federal Act on Data Protection) into the Cloud Service, Customer agrees to first obtain the consent (in the sense of Art. 6 para. 2, lit. b. of the Swiss Federal Act on Data Protection) of such legal entity (**"Data Subject"**) before using the Cloud Service, as described herein, for such Data Subject(s). SAP agrees to afford to such personal data a similar level of protection as set forth in Sections 2, 3 and 6 of this Schedule.

(g) **Turkey.** To the extent a Data Controller in Turkey or its Authorized Users intend to enter Personal Data into the Cloud Service, Customer agrees to first obtain the consent of each Data Subject to an International Transfer as contemplated under this Schedule if and to the extent required under the applicable data protection law in Turkey. Customer hereby confirms and commits that it has received the Personal Data and informed the related persons regarding the transfer/process of the Personal Data in accordance with the applicable law.

(h) **United States**. Unless SAP and Customer have executed a so called Business Associate agreement for the exchange of protected health information (**"PHI"**) as defined in the United States Health Insurance Portability and Accountability Act of 1996, as amended, in relation to the Cloud Service, Customer hereby represents that Customer will not submit PHI to the Cloud Service nor solicit such information from partners or customers as part of use of the Cloud Service.

6. CERTIFICATIONS AND AUDITS

6.1 Certifications and Audit Reports.

For the production systems which run the Cloud Service and during the term of the Agreement SAP shall maintain, at its own expense, applicable certifications or audit reports:

(a) As a minimum, SAP engages an internationally recognized independent third party auditor to review the measures in place in protection of the Cloud Service: (i) Certifications may be based on ISO 27001 or other standards (scope as defined in certificate). (ii) For certain SAP Cloud Services, SAP additionally provides a valid ISAE3402 or SSAE16-SOC 1 Type 2 and/or ISAE3000 or SSAE16-SOC 2 Type 2 report. Upon Customer's request, SAP shall inform Customer about the applicable certifications and audit standards available for the Cloud Service concerned.

(b) Upon Customer's request, SOC-Audit reports or ISO certifications are available through the third party auditor or SAP, as applicable.

6.2 Customer Audits.

Subject to Section 6.4 below and as required under the mandatory Data Protection Law, Customer (or an independent third party auditor on its behalf that is subject to confidentiality obligations consistent with those in the Agreement) may audit SAP's control environment and security practices relevant to Personal Data processed hereunder for Customer in any of the following events:

(a) SAP has not provided sufficient evidence of its compliance under Section 6.1,

(b) An event set out in Section 3.6 above has occurred,

(c) Customer or another Data Controller has reasonable grounds to suspect that SAP is not in compliance with its obligations under this Schedule,

(d) A further audit is required by Customer's or another Data Controller's data protection authority or regulator (e.g. in case a law enforcement agency has the right to audit a Data Controller if the Personal Data was processed at the premise of the Data Controller).

6.3 Cooperation.

SAP shall reasonably support Customer throughout its verification processes required under the Data Protection Law and provide Customer with the necessary information.

6.4 Audit Restrictions.

(a) Unless required by mandatory Data Protection Law, an audit pursuant to Section 6.2 is limited to once in any twelve-month period.

(b) An audit may not exceed three business days.

(c) Customer shall provide SAP with reasonable prior written notice (at least 60 days unless a data protection authority requires Customer's earlier control under mandatory Data Protection Law).

(d) Customer and SAP shall mutually agree the scope and determine the agenda of the audit in advance. The audit shall, to the extent possible, rely on certifications and audit reports or other verifications available to confirm SAP's compliance with this Schedule and exclude any repetitive audits.

(e) Customer shall conduct the audit under reasonable time, place and manner conditions and provide SAP with a copy of the audit report.

(f) Each party shall bear its own costs for an audit under Section 6.2 except that Customer shall bear also SAP's costs of SAP's internal resources required to conduct any audit under Section 6.2 (d) or under mandatory Data Protection Law. SAP's internal costs shall be based on the then-current daily professional service rates as applicable to Customer or, in lack of such agreement, on SAP's price list.

(g) If an audit determines that SAP has breached its obligations under this Schedule (a **"Finding"**) SAP shall promptly remedy such Finding. It is at SAP's sole discretion to determine which measures are best suitable to ensure compliance under this Schedule.

7. DEFINITIONS

Any capitalized terms used herein, such as Affiliates, Agreement, Customer, Authorized User (sometimes also referred to as User or Named User), Order Form or Cloud Service (sometimes also referred to as Service), shall have the meaning given to them in the Agreement.

7.1 **"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.

7.2 **"Data Controller"** has the meaning given to this term under the applicable Data Protection Law.

7.3 **"Data Exporter"** as used in the Standard Contractual Clauses means Customer as listed in an Order Form or its Data Controller(s).

7.4 **"Data Importer"** as used in the Standard Contractual Clauses means the applicable Non-EEA Entity.

7.5 **"Data Processor"** has the meaning given to this term under the applicable Data Protection Law.

7.6 **"Data Protection Law"** means the legislation protecting the fundamental rights and freedoms of persons and, in particular, their right to privacy, with regard to the processing of Personal Data under the Agreement. SAP shall comply with additional obligations set out in an Order Form that are required under compelling local data protection laws applicable to SAP as the Data Processor.

7.7 **"Data Subject"** means and identified or identifiable individual or a legal entity (where so defined under the applicable Data Protection Law).

7.8 **"EEA"** means the European Economic Area as well as any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

7.9 **"European Subprocessor"** means a Subprocessor that is physically processing Personal Data in the EU, Iceland, Liechtenstein, Norway, or Switzerland.

7.10 **"Non-EEA Entity"** means any SAP entity or Subprocessor incorporated outside the EEA, i.e. in a country, which does not provide an adequate level of data protection as determined by the European Commission.

7.11 **“Personal Data”** has the meaning given to that expression in the Data Protection Law and, for the purposes of this Schedule, includes only such personal data entered by Customer or its Authorized Users into or derived from their use of the Cloud Service or supplied to or accessed by SAP or its Subprocessors in order to provide support in accordance with the Agreement. Personal Data is a sub-set of Customer Data and used herein when any Data Protection Law applies.

7.12 **“SAP”** means the SAP entity that is the party to the Order Form that incorporates this Schedule.

7.13 **“Security Breach”** means any acts or omissions by SAP or its Subprocessors that led to an unauthorized disclosure of Personal Data in breach of the measures set forth in Appendix 2 or similar incident for which the Data Controller is legally required to provide notice to the Data Subject or the data protection authority concerned.

7.14 **“Standard Contractual Clauses”** or sometimes also referred to the “EU Model Clauses” means the (Standard Contractual Clauses (processors)) based on the Commission Decision of 5 February 2010, on standard contractual clauses for the transfer of Personal Data to processors established in third countries, under Directive 95/46/EC (notified under document number C(2010) 593), or any subsequent version thereof released by the Commission (which shall automatically apply), including Appendices 1 and 2 attached hereto.

7.15 **“Subprocessor”** as used in the Standard Contractual Clauses and this Schedule means the SAP Affiliates and third party subprocessors engaged by SAP or SAP’s Affiliates in accordance with Section 4.

8. EU ACCESS (OPTION)

8.1 Eligible Cloud Service.

In deviation of Section 5.1 of this Schedule, SAP agrees to provide EU Access for the Cloud Service if and to the extent agreed on the Order Form. Customer understands that EU Access is provided only for EU Access eligible services, as determined by SAP, that are hosted by SAP in the EU.

8.2 Data Center Location.

Upon the Order Form Effective Date and in deviation of any conflicting provision in the Order Form, the Data Centers used to host Personal Data in the ordered Cloud Service are located in the territory of the EEA or Switzerland. SAP undertakes not to migrate the Customer instance to a Data Center outside the territory of 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 shall notify Customer in writing (email permitted) thereof no later than thirty days before the planned migration.

8.3 EU Access.

Customer has requested and SAP has agreed to refrain from using Subprocessors other than European Subprocessors in providing support of the production systems of the Cloud Service to the extent such support may require access to Personal Data whether or not such access occurs.

8.4 Exclusion.

The following Personal Data is not subject to EU Access:

(a) Contact details of the sender of a support and/or incident ticket, notice or message when filing a support and/or incident ticket

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

(c) Personal Data in non-production systems.

Personal Data that is not subject to EU Access shall only be transferred or accessed by SAP or its Subprocessors in accordance with Section 5.

Attachment 1
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)[1]

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Customer and/or Customer Affiliates based in the EU in the sense of Section 1.2 (b) of the DATA PROCESSING AGREEMENT (in the Clauses hereinafter referred to as the '**data exporter'**)

and

SAP SE as representative for Non-EEA Entities in the sense of Section 5.2 of the DATA PROCESSING AGREEMENT (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;
(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.

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

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 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

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. 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, namely Germany.

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.

APPENDIX 1 TO DATA PROCESSING AGREEMENT AND STANDARD CONTRACTUAL CLAUSES

The parties may provide further details in an Order Form or the Supplement, if required, or adjusted in the description below by Customer.

Data Exporter

The Data Exporter subscribed to a SAP Cloud Service which allow Authorized Users to enter, amend, use, delete or otherwise process Personal Data as contemplated under the Agreement.

Data Importer

SAP and its Subprocessors provide the Cloud Service which includes the following Support:
SAP Affiliates around the world support the global SAP Cloud Service data centers remotely from SAP facilities, e.g. in St. Leon/Rot (Germany), India and other locations where SAP employs personnel in the Operations/Cloud Delivery function. Support includes but is not limited to:

- Monitoring the Cloud Service and underlying infrastructure
- Backup & restore Customer Data stored in the Cloud Service
- Release and development of patches, new updates and upgrades to the Cloud Service and underlying infrastructure
- Troubleshooting for servers, storage, network equipment
- Database monitoring, troubleshooting, day-to-day database administration activities incl. production database sizing, index creation, performance tuning, patch management. Standby database management and projects related to database functions
- Security monitoring, network-based intrusion detection support, conducting penetration tests

SAP Affiliates provide also 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 (incident): SAP answers phones and performs basic troubleshooting and routes and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data subjects

The Personal Data transferred concern the following categories of data subjects:
Unless provided otherwise by Data Exporter, Data Subjects may include employees, contractors, business partners or other individuals whose Personal Data is stored in the Cloud Service.

Categories of data

The Personal Data transferred concern the following categories of data:
Customer determines the categories of data per Cloud Service subscribed. Customer's data fields can be configured as part of the implementation of the Cloud Service or as otherwise permitted in the Cloud Service. The Personal Data transferred usually concern (a subset of) 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 which Authorized Users enter into the Cloud Service including bank account data, credit or debit card data.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data: As set out in the Order Form, if any.

Processing operations

The Personal Data transferred will be subject to the following basic processing activities:

- use of Personal Data to provide the Cloud Service (including Operational and Technical Support)
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any patch, update, upgrade / new releases 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, if required

APPENDIX 2 TO DATA PROCESSING AGREEMENT AND STANDARD CONTRACTUAL CLAUSES

1. PREAMBLE

1.1 Deviations.

Some Cloud Services are subject to different support terms, as set forth in the respective Supplement or Order Form.

1.2 Scope.

In all other cases, the description of the technical and organizational security measures set out in Section 2 below implemented by the Data Importer for Personal Data stored in the production system of the Cloud Service (in accordance with Clauses 4(d) and 5(c) of the Standard Contractual Clauses) shall apply.

2. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define the current security measures established by SAP.

2.1 Physical Access Control.

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located which process and/or use Personal Data.

Measures:

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 ensure proper functionality, physical security equipment (e.g. motion sensors, cameras, etc.) are maintained on a regular basis. In detail, the following physical security measures are implemented at all Data Centers:

(a) SAP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.

(b) In general, buildings are secured through access control systems (smart card access system).

(c) As a minimum requirement, the outermost shell of the building must be fitted with a certified key system including modern, active key management.

(d) Depending on the security classification, buildings, individual areas and surrounding premises are further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.

(e) Access rights will be granted to authorized persons on an individual basis according to the System and Data Access Control measures set out 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 and all third party Data Center providers are logging the names and times of persons entering the private areas of SAP within the Data Centers.

(f) SAP employees and external personnel must wear their ID cards at all SAP locations.

2.2 System Access Control.

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

Measures:

(a) Multiple authorization levels are used to grant access to sensitive systems including those storing and processing Personal Data. Processes are in place to ensure that only authorized users have the appropriate authorization to add, delete, or modify users.

(b) All users access SAP's systems with a unique identifier (user ID).

(c) SAP has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user changes roles or leaves the company, its access rights are revoked.

(d) SAP has established a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, 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 case of domain passwords, the system forces a password change every six months complying with the requirements for complex passwords. Each computer has a password-protected screensaver.

(e) Remote access to the Cloud Service delivery environment requires at least strong authentication mechanisms (for instance a combination of a password and an additional security feature). Passwords with a minimum length of fifteen (15) characters must be used for administrative accounts and service accounts of security-critical IT systems. New passwords must be different from an Authorized User's last five (5) passwords. The company network is protected from the public network by firewalls.

(f) SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts) and on all file servers and all workstations.

(g) A security patch management is implemented to ensure deployment of relevant security updates.

(h) Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

2.3 Data Access Control.

Persons entitled to use data processing systems shall 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:

(a) Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. SAP uses authorization concepts that document how authorizations are assigned and which authorizations are assigned. All personal, confidential, or otherwise sensitive data is protected in accordance with the SAP security policies and standards.

(b) All production servers of any SAP Cloud Service are operated in the relevant Data Centers/server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on the IT systems.

(c) SAP does not allow the installation of personal software or other software not approved by SAP to systems being used for any Cloud Service.

(d) A SAP security standard governs how data and data carriers are deleted or destroyed.

2.4 Data Transmission Control.

Personal Data must not be read, copied, modified or removed without authorization during transfer.

Measures:

(a) Where data carriers are physically transported, adequate measures are implemented at SAP to ensure the agreed service levels (for example, encryption, and lead-lined containers).

(b) Personal Data transfer over SAP internal networks are protected as any other confidential data according to SAP Security Policy.

(c) When the data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed in the Agreement. This applies to both physical and network based data transfer. In any case the Customer assumes responsibility for any data transfer from SAP's Point of Demarcation (e.g. outgoing firewall of the SAP Data Center which hosts the Cloud Service).

2.5 Data Input Control.

It shall be possible to retrospectively examine and establish whether and by whom at SAP Personal Data have been entered, modified or removed from data processing systems used to provide the Cloud Service.

Measures:

SAP only allows authorized persons to access Personal Data as required in the course of their work. SAP implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its Subprocessors to the greatest extent supported by the Cloud Service.

2.6 Job Control.

Personal Data being processed on commission shall be processed solely in accordance with the Agreement and related instructions of the Customer.

Measures:

(a) SAP uses controls and processes to ensure compliance with contracts between SAP and its customers, Subprocessors or other service providers.

(b) As part of the SAP Security Policy, Customer Data requires at least the same protection level as “confidential” information according to the SAP Information Classification standard.

(c) All SAP employees and contractual partners are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

2.7 Availability Control.

Personal Data shall be protected against accidental or unauthorized destruction or loss.

Measures:

(a) SAP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.

(b) SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.

(c) SAP has defined contingency plans as well as business and disaster recovery strategies for Cloud Services.

(d) Emergency processes and systems are regularly tested.

2.8 Data Separation Control.

Personal Data collected for different purposes can be processed separately.

Measures:

(a) SAP uses the technical capabilities of the deployed software (for example: multi-tenancy or separate system landscapes) to achieve data separation between Personal Data from one and any other customer.

(b) SAP maintains dedicated instances (with logical or physical separation) for each Customer.

(c) Customers (including their Affiliates) have access only to own Customer instance(s).

2.9 Data Integrity Control.

Ensures that Personal Data will remain intact, complete and current during processing activities:

Measures:

SAP has implemented a defense strategy in several layers as a protection against unauthorized modifications. This refers to controls as stated in the control and measure sections as described above. In particular:

(a) Firewalls;
(b) Security Monitoring Center;
(c) Antivirus software;
(d) Backup and recovery;
(e) External and internal penetration testing;
(f) Regular external audits to prove security measures.