DATA PRIVACY AND SECURITY – DATA CONTROLLER TO DATA PROCESSOR AGREEMENT

This document **("Exhibit")** shall become an integral part of the Order Form signed by Customer (the "Agreement") referring to these terms. This Exhibit serves as a written commissioned data processing agreement between SAP and each **Data Controller** providing **Personal Data** in connection with its use of the Service and furthermore defines the applicable technical and organizational measures SAP implements and maintains to protect **Personal Data** stored in the Service. The written form of this Exhibit shall be deemed to be evidenced upon SAP's receipt of any of the following: (i) signed original Order Form; (ii) signed Order Form in pdf or similar format; (iii) accepted Order Form using DocuSign or a similar product used by SAP to receive an Order Form from Customer.

Customer acts as the **Data Controller** concerning **Personal Data** of its own Named Users as well as on behalf of and in the name of its Affiliates or third parties in their capacity as **Data Controllers** of Named Users authorized by Customer to use the Service. Customer shall enter into data processing agreements with its **Data Controllers** that are required to allow SAP (as **Data Processor** or **Subprocessor**, as the case may be) and its **Subprocessors** to process any **Personal Data** as described in this Exhibit. 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 Customer.

If any provision of this Exhibit 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 Exhibit, and all provisions not affected by such invalidity shall remain in full force and effect.

1. Data Processing Purposes

1.1 Customer and its Affiliates, as the respective **Data Controller(s)**, shall determine the purposes of collecting, processing, and otherwise using **Personal Data** stored in the Service. Unless provided otherwise in the Agreement, **Appendix 1** of the **Standard Contractual Clauses** and the Exhibit shall apply to such data processing.

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

a) Setting up, operating, monitoring and providing the 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 Named Users and other administrative purposes as clarified in the terms associated with a particular Service and
e) Executing instructions of the Customer in accordance with Sections 2.1 and 2.2 below.

2. SAP Obligations

2.1 SAP shall process **Personal Data** only in accordance with the **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 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.

2.2 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 Service does not allow the Customer, its **Data Controllers** or Named Users to do so. In the event that SAP needs to access any of Customer's systems or Customer's instance of the 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.

2.3 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 applicable **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.

2.4 SAP shall, as a minimum, implement and maintain appropriate technical and organizational measures as described in **Appendix 2** of the Exhibit to keep **Personal Data** secure and protect it against unauthorized or unlawful processing and accidental loss, destruction or damage. Since SAP provides the 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 Service. Customer understands and agrees that the technical and organizational measures are subject to technical progress and development. In that regard, SAP is expressly allowed to implement adequate alternative measures as long as the security level of the measures is maintained. In the event of any detrimental change SAP shall provide a notification together with any necessary documentation to Customer by email or publication on a website easily accessible by Customer.

2.5 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 2.1 above.

2.6 SAP shall promptly inform Customer as soon as it becomes aware of serious disruptions of the processing operations, reasonable suspected or actual data protection violations 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.

2.7 At Customer's 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. Subprocessors

3.1 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**") to the extent necessary for fulfilling its contractual obligations under the Agreement 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. 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 Exhibit. SAP undertakes to have a selection process by which it evaluates the security, privacy and confidentiality practices of a **Subprocessor** in regard 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).

3.2 SAP will inform Customer upon its request by email about the name, address and role of each **Subprocessor** it uses to provide the Service. SAP may remove or appoint suitable and reliable other Subprocessors at its own discretion in accordance with this Section 3. SAP will inform Customer by email in advance (except for **Emergency Replacements** under Section 3.3) of any changes to the list of **Subprocessors**, which shall be deemed accepted as long as they comply with and are bound by applicable **Data Protection Law** or, if a **Subprocessor** is incorporated outside the EEA, the **Standard Contractual Clauses**. If Customer has a legitimate reason to object to SAP's use of a **Subprocessor** (e.g. if the **Subprocessor** is located in a country without an adequate level of data protection 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 (30) days after receipt of SAP's notice. If Customer does not object during such time period the new **Subprocessor**(s) shall be deemed accepted. 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): (a) SAP will abort its plans to use the **Subprocessor** with regard to **Personal Data**; or (b) 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 (c) SAP may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the 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 (30) days after SAP's receipt of Customer's objection, either party may terminate the affected Service with reasonable prior written notice.

3.3 "**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 the process to formally appoint such **Subprocessor** pursuant to Section 3.2 shall be triggered.

4. International Transfers and Country-Specific Deviations

4.1 **Personal Data** that SAP has received from any **Data Controller** hereunder shall only be exported by SAP or its **Subprocessors** from the Data Center 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) when a **Non-EU Entity** fulfills the requirements of Section 4.2 below. The same shall apply to SAP receiving **Personal Data** directly from a **Data Controller** in the EEA, via Internet access to a Service hosted in a Data Center outside the EEA.

4.2 SAP (through SAP SE) has entered into the **Standard Contractual Clauses** with each **Non-EU Entity** processing **Personal Data** hereunder by means of an **International Transfer**. Customer hereby accedes to the **Standard Contractual Clauses** and may then directly enforce them against the relevant Non-EU Entity. Customer furthermore will procure that each Data Controller will accede to such **Standard Contractual Clauses** entered into between SAP and Customer. In the event such direct right 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 Exhibit. Unless otherwise agreed by the parties, Appendices 1 and 2 of the **Standard Contractual Clauses** as attached shall apply. Nothing in the Agreement shall be construed to prevail over any conflicting Clause of the **Standard Contractual Clauses**. Customer acknowledges it has had the opportunity to review the **Standard Contractual Clauses** or to obtain a full copy from SAP.

4.3 The **Standard Contractual Clauses** shall be governed by the law of the Member State in which the EEA based **Data Exporter** is established.

4.4 **Switzerland.** To the extent a **Data Controller** in Switzerland or its **Named Users** intend to enter personal data of legal entities (also considered personal data under the Swiss Federal Act on Data Protection) into the 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 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 1, 2 and 5 of this Exhibit.

4.5 **Austria**. To the extent a **Data Controller** in Austria or its **Named 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 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 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 1, 2 and 5 of this Exhibit.

4.6 **Russian Federation**. The parties agree that SAP is accepting from the Customer certain **Personal Data** of Russian Citizens for storing and shall ensure availability of such stored **Personal Data** to the extent technically feasible for the Customer's own processing. Customer or Customer Affiliates **as Data Controllers** remain operators of **Personal Data** 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 Services which involve processing of Russian citizen's **Personal Data** and (ii) whether Services can be used inside or outside the Russian Federation.

4.7 **Turkey.** To the extent a **Data Controller** in Turkey or its **Named Users** intend to enter **Personal Data** into the Service, Customer agrees to first obtain the consent of each **Data Subject** to an **International Transfer** as contemplated under this Exhibit if and to the extent required under the applicable data protection law in Turkey. The 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.

4.8 **United States**. Unless SAP and Customer have executed a 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

Service, Customer hereby represents that Customer will not submit PHI to the Service nor solicit such information from partners or customers as part of use of the Service.

4.9 South Korea. To the extent a **Data Controller** in Republic of Korea or its **Named Users** intend to enter **Personal Data** into the Service, Customer agrees to first obtain the consent of each **Data Subject** to an **International Transfer** as contemplated under this Exhibit if and to the extent required under the applicable Personal Information Protection Act in Republic of Korea. The 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.

5. Monitoring Rights of Customer

5.1 For the production systems which run the Service itself and during the term of the Agreement SAP shall maintain, at its own expense, applicable certifications or audit reports. Unless provided otherwise in a Supplement, SAP engages an internationally recognized independent third party auditor to review the measures in place in protection of the Service(s). Certifications may be based on ISO 27001 or other standards (scope as defined in certificate). For certain SAP Cloud Services, SAP performs regular audits (at least annually) via certified auditors to provide a valid SOC 1 Type 2 (SSAE 16 or ISAE 3402) and/or SOC 2 Type 2 report. Audit reports are available through the third party auditor or SAP, as applicable. Upon Customer's request, SAP shall inform the Customer about the applicable certifications and audit standards available for the Service concerned.

5.2 If SAP fails to perform its audit obligations under Section 5.1 and has not provided sufficient evidence of its compliance after Customer's written request, 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 once in any twelve (12)-month period, with reasonable prior written notice (at least 60 days unless a data protection authority requires Customer's earlier control under applicable **Data Protection Law**) and under reasonable time, place and manner conditions.

5.3 Furthermore, (i) following an event set out in Section 2.6 above, or (ii) if Customer or another **Data Controller** has reasonable ground to suspect the non-compliance of SAP with its obligations under this Exhibit, or (iii) if a further audit is required by Customer's or another **Data Controller's** data protection authority, 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 accordance with applicable **Data Protection Law**.

5.4 SAP shall reasonably support Customer throughout these verification processes and provide Customer with the required information. Customer shall bear any costs (including SAP's internal resource based on then-current daily professional service rates per SAP's price list) for any efforts on SAP's side exceeding more than 4 hours per year.

Definitions

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

"Data Center" means the location where the production instance of the Cloud Services 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.

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

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

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

"Data Processor" has the meaning given to this term in the applicable Data Protection Law.

"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 by a data processor both in the EEA and, if different, such legislation of the country where the data center is located. SAP may agree in an Order Form to comply with other compelling local data protection laws applicable to SAP as the Data Processor, if and to the extent agreed.

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

"EEA" means the European Economic Area.

"Non-EU Entity" means any SAP entity or Subprocessor incorporated in a country which does not provide an adequate level of data protection according to European Union (EU) laws and regulations.

"Personal Data" has the meaning given to that expression in the Data Protection Law and, for the purposes of this Exhibit, includes only such personal data entered by Customer or its Named Users into or derived from their use of the 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.

"SAP" means the SAP entity that is the party to the Order Form.

"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.

"Standard Contractual 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.

"Subprocessor" as used in the Standard Contractual Clauses and this Exhibit means the SAP Affiliates and third party subprocessors engaged by SAP or SAP's Affiliates in accordance with Section 3.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES AND THE EXHIBIT

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** is:

The **Data Exporter** subscribed to certain SAP Cloud Services which allow its Named Users to enter, amend, use, delete or otherwise process **Personal Data** as contemplated under the Agreement.

Data Importer
The **Data Importer** is:

SAP and its Subprocessors provide certain Cloud Services which include the hosting of the Service and the provision of technical support to Customer, its Affiliates and their respective Named Users as contemplated under the Agreement.

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 Service.

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

Customer determines the categories of data per Service subscribed. Customer's data fields can be configured as part of the implementation of the Service or as otherwise permitted in the 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 Customers' Named Users enter into the 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 notified by Customer.

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

- use of **Personal Data** to provide the Service and to provide assistance to technical support
- storage of **Personal Data** in dedicated Service data centers (multi-tenant architecture)
- upload any patch, update, upgrade / new releases to the 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 THE STANDARD CONTRACTUAL CLAUSES AND THE EXHIBIT

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

In all other cases, the description of the technical and organizational security measures (TOMs) implemented by the Data Importer for Personal Data in accordance with Clauses 4(d) and 5(c) shall apply:

1. Technical and Organizational Measures

The following sections define the current security measures established by SAP. SAP may change these at any time without notice by keeping a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

1.1 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**:

- SAP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- In general, buildings are secured through access control systems (smart card access system).
- As a minimum requirement, the outermost shell 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 are further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights will be 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 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**.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

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

- Multiple authorization levels are used to grant access to sensitive systems including those storing and processing **Personal Data**. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
- All users access SAP's systems with a unique identifier (user ID).
- 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 leaves the company, its access rights are revoked.
- 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.
- 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) and on all file servers and all workstations.
- A security patch management is implemented to ensure 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 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:

- 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.
- 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.
- SAP does not allow the installation of personal software or other software not approved by SAP to systems being used for any Cloud Service.
- A SAP security standard governs how data and data carriers are deleted or destroyed.

1.4 Data Transmission Control:
Personal Data must not be read, copied, modified or removed without authorization during transfer.
Measures:
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).
Personal Data transfer over SAP internal networks are protected as any other confidential data according to SAP Security Policy.
When the data is being transferred between SAP and its customers, the protection measures for the transferred **Personal Data** are mutually agreed upon and made 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 from SAP's Point of Demarcation (e.g. outgoing firewall of the SAP Data Center which hosts the Cloud Service).

1.5 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.

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

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

1.7 Availability Control:
Personal Data shall be protected against accidental or unauthorized destruction or loss.
Measures:

- SAP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the **Data Centers**.
- SAP has defined contingency plans as well as business and disaster recovery strategies for Cloud Services.
- Emergency processes and systems are regularly tested.

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

- SAP uses the technical capabilities of the deployed software (for example: multi-tenancy or separate system landscapes) to achieve data separation between **Personal Data** from one and any other customer.
- SAP maintains dedicated instances for each Customer.
- Customers (including their Affiliates) have access only to own Customer instance(s).

1.9 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:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;

Regular external audits to prove security measures.