Technical and Organizational Measures (TOMs) for SAP Cloud Services

The following sections define SAP's current technical and organizational measures and are incorporated into Schedule 2 of the DPA. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. PHYSICAL ACCESS CONTROL

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

1.1. Measures

1.1.1. SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy.

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

1.1.3. As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.

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

1.1.5. Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see 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.

1.1.6. SAP employees and external personnel must wear their ID cards at all SAP locations.

1.2. Additional measures for data centers

1.2.1. All data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the data center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

1.2.2. SAP and all third-party data center providers log the names and times of authorized personnel entering SAP's private areas within the data centers.

2. SYSTEM ACCESS CONTROL

Data processing systems used to provide the Cloud Service must be prevented from being used without authorization by taking the following measures:

2.1. Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy

2.2. All personnel access SAP's systems with a unique identifier (user ID).

2.3. SAP has procedures in place so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.

2.4. SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

2.5. The company network is protected from the public network by firewalls.

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

2.7. Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

3. DATA ACCESS CONTROL

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

3.1. As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.

3.2. Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.

3.3. All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.

3.4. SAP does not allow the installation of software that has not been approved by SAP.

3.5. An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

4. DATA TRANSMISSION CONTROL

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

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

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

5. DATA INPUT CONTROL

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems. SAP takes the following measures:SAP only allows authorized personnel to access Personal Data as required in the course of their duty.

SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its Subprocessors within the Cloud Service to the extent technically possible.

6. JOB CONTROL

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer. SAP takes the following measures:

6.1. SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.

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

6.3. All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

7. AVAILABILITY CONTROL

Personal Data will be protected against accidental or unauthorized destruction or loss.SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary. SAP takes the following measures:

7.1. SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the data centers.

7.2. SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.

7.3. Emergency processes and systems are regularly tested.

8. DATA SEPARATION CONTROL

Personal Data collected for different purposes can be processed separately. SAP takes the following measures:

8.1. SAP uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.

8.2. Customer (including its Controllers) has access only to its own data.

8.3. If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

9. DATA INTEGRITY CONTROL

Personal Data will remain intact, complete and current during processing activities. SAP takes the following measures:

9.1. SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

9.2. In particular, SAP uses the following to implement the control and measure sections described above:

9.3. Firewalls;

9.4. Security Monitoring Center;

9.5. Antivirus software;

9.6. Backup and recovery;

9.7. External and internal penetration testing;

9.8. Regular external audits to prove security measures.