Exhibit 2

TECHNICAL AND ORGANIZATIONAL MEASURES

This Exhibit 2 (Technical and Organizational Measures) is incorporated by reference into the CDPA as Exhibit 2 and describes three possible processing scenarios and the minimum requirements Contractor must implement for each scenario. The applicable scenario for the Service will be agreed in the DP Annex. Details or deviations, if any, must be agreed in an DP Annex to this CDPA.

Rationale for differing scenarios: In some scenarios, the responsibility for ensuring the TOMs may not be in the sole responsibility of Contractor. For example, where Contractors provide support services solely on SAP's premise, SAP is responsible for the physical security of the buildings. However, Contractors who provide Cloud Services would control all aspects of the TOMs listed. The following table outlines the typical scenarios for the provisioning of Services:

Definition of scenarios:

Scenarios	**Location** **Where are services provided?**	**IT-systems/-infrastructure** **In which systems are services provided?**
Scenario I	Services provided also from own/rented premises/offices of the Contractor or its Subprocessors (including home office).	Service provisioning includes the processing and storage of personal data also in systems/ infrastructure of the Contractor or its Subprocessors.
Scenario II	Services provided also from own/rented premises/offices of Contractor or its Subprocessors (including home office).	Services provided exclusively in systems / infrastructure of SAP (including remote access via SAP WTS(Citrix) and/or Other Controllers (including remote access granted by other controllers, e.g. VPN, etc.)
Scenario III	Services provided exclusively from SAP premises and/or Other Controller premises (e.g. onsite at customers of data exporter)	Services provided exclusively in systems/ infrastructure of SAP (including remote access via SAPWTS(Citrix) and/or Other Controllers (including remote access granted by other controllers, e.g. VPN, etc.)

With respect to these scenarios, tables at the end of the individual TOMs described hereinafter indicate Data Importer's responsibility (fields marked with an "X").

Access Control

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process Personal Data; persons are unauthorized if their activity does not correspond to tasks assigned to them. Exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by the Data Importer and do not get access to the personal data themselves.

Including, without limitation, the data importer must:

Access Control	**Scenarios**		
	I	**II**	**III**
Specify authorized individuals	X	X	
Use an access control process to avoid unauthorized access to your company's premises	X	X	
Have an access control process to restrict access to data centres / rooms where data servers are located	X		
Use video surveillance and alarm devices with reference to access areas	X	X	

Personnel without access authorization (e.g. technicians, cleaning personnel) must be accompanied all times	X	X	

System Access Control

Data processing systems must be prevented from being used without authorization.

Including, without limitation, the Data Importer must:

System Access Control	**Scenarios**		
	I	**II**	**III**
Ensure that all computers processing personal data (this includes remote access) are password protected			
after boot sequences	X	X	X
when left even for a short period	X	X	X
to prevent unauthorized persons from accessing any personal data			
Have dedicated user IDs for authentication against systems user management for every individual	X		
Assign individual user passwords for authentication	X		
Ensure that the access control is supported by an authentication system	X		
Only grant system access to data importer's authorized personnel and/or to permitted employees of data importer's subcontractors and strictly limit such person's access to applications which process personal data as required for those persons to fulfil their function	X		
Implement a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords	X		
Ensure that passwords are always stored in encrypted form	X		
Have a proper procedure to deactivate user account, when user leaves company or function	X		
Have a proper process to adjust administrator permissions, when an administrator leaves company or function	X		

Access Control to Personal Data

Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing.

Including, without limitation, the data importer must:

Access Control to Personal Data	**Scenarios**		
	I	**II**	**III**
Restrict access to files and programs based on a "need-to-know-basis"	X		
Store data carriers in secured areas	X		
Only grant access to Data importer personnel and assigns minimal permissions to access data as needed to fulfil their function	X		

Data Transmission Control

Data transmission control is addressed in the SAP Supplier Security Standard Terms, available at https://www.sap.com/docs/download/agreements/supplier-portal/general-terms-and-conditions-for-procurement/sap-supplier-security-standard-terms-global.pdf

Data Entry Control

It shall be possible retrospectively to examine and establish whether and by whom Personal Data have been entered into data processing systems, modified or removed.

Including, without limitation, the Data Importer must:

Data Entry Control	**Scenarios**		
	I	**II**	**III**
Log administrators and user activities	X		
Permit only authorized personnel to modify any personal data within the scope of their function	X		

Job Control

Personal Data being processed on commission shall be processed solely in accordance with the CDPA and the service schedule and instructions of the Controller.

Including, without limitation, the Data Importer must:

Job Control	**Scenarios**		
	I	**II**	**III**
Establish controls of the contractual performance	X	X	X
Work according written instructions or contracts	X	X	X
Process the Personal Data received from different clients to ensure that in each step of the processing the Controller of Personal Data can be identified, so data is always physically or logically separated	X		

Availability Control

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

Including, without limitation, the data importer must:

Availability Control	**Scenarios**		
	I	**II**	**III**
Create back-up copies stored in specially protected environments	X		
Perform regular restore tests from those backups	X		
Create contingency plans or business recovery strategies	X		
Not use Personal Data for any purpose other than what have been contracted to perform	X	X	X
Not remove Personal Data from Data importer's business computers or premises for any reason (unless data exporter has specifically authorized such removal for business purposes).	X	X	X
To use only authorized business equipment to perform the Services	X		
Whenever a user leaves its desk unattended during the day and prior to leaving the office at the end of the day, he/she must ensure that documents containing personal data are placed in a safe and secure environment such as a locked desk drawer, filing cabinet, or other secured storage space. (clean desk)	X	X	
Implement a process for secure disposal of documents or data carriers containing Personal Data	X	X	
Have firewalls on network level to prevent unauthorized access to systems and services on network level	X		
Ensure, that each computer system runs an up to date antivirus solution	X	X	X

Organizational Requirements

The internal organization of the Data Importer shall meet the specific requirements of data protection. In particular, the Data Importer shall take TOMs to avoid the accidental mixing of Personal Data.

Including, without limitation, the Data Importer must:

Organizational Requirements	**Scenarios**		
	I	**II**	**III**
Designate a data protection officer (or a responsible person if a data protection officer is not required by law)	X	X	X
Get the written commitment of the employees to maintain confidentiality	X	X	X
Process the Personal Data received from different clients to ensure that in each step of the processing the respective client can be identified, so data is always physically or logically separated	X		