APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

The parties may provide further details in an offering agreement for the Services, if required.

Data exporter

The data exporter is an entity (the "IBM Customer") that has contracted with an affiliate of the data importers (the "IBM Contracting Party") for SaaS services which allow its Named Users to enter, amend, use, delete or otherwise process **Personal Data.**

Data importer

The data importers are affiliates of the IBM Contracting Party, which provide information technology services in respect to the Services.

Data subjects

Unless instructed otherwise by the Data Exporter, data subjects may include the IBM Customer's and its affiliates' employees, contractors, business partners, or other individuals whose Personal Data is processed by the Services.

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. Identified representatives of the customer determine what personal information is captured based on their business processes and corresponding use of the service. The Personal Data transferred across all IBM offerings 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 and company name.

Special categories of data (if appropriate)

The **Personal** Data transferred concern the following special categories of data:

None.

Please notes, these are Sample EU Model Clause agreement appendices to be used as a reference for what is in the IBM SaaS EU Model Clause appendices. These are sample documents intended to be used for illustration and are not to be used as part of a transaction. The IBM contracts process will include the official model clause document.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The data importers and the IBM Contracting Party (as defined in Appendix 1) implement and maintain the following practices and procedures, which may be revised periodically, regarding the systems used to host and operate the Services (as defined in Appendix 1):

Security Policies

IBM security policies and standards are reviewed regularly and refined as necessary to keep current with modern threats and in line with international standards updates.

IBM security incidents are handled in accordance with our comprehensive incident response procedures, taking into account any data breach notification requirements under applicable law.

IBM employees are provided with security education and are required to certify annually that they will comply with IBM's ethical business conduct, confidentiality, and security requirements, as set out in IBM's "Business Conduct Guidelines."

Access, Intervention, Transfer and Separation Control

Access to client data (including any personal data) is allowed only by authorized personnel in accordance with principles of segregation of duties, strictly controlled under IBM's identity and access management policies, and monitored in accordance with IBM's internal privileged user monitoring and auditing program.

IBM's privileged access authorization is individual, role-based, and subject to regular validation.

Access to client data is only granted as necessary to deliver services and support to the client (i.e., least required privilege).

Transfer of data within IBM's network takes place behind IBM's firewalls. Wi-Fi is not used within IBM production data centers.

The IBM SaaS offerings maintain logical separation of client data. Internal rules and measures are in place to segregate data processing (i.e., storage, change, copy, delete and/or transfer data) and storage media based on the contracted purposes.

Service Integrity & Availability Controls

Modifications to operating system resources and application software are governed by IBM's rigorous change management process. Changes to firewall rules are also governed by the change management process and are separately reviewed by IBM security staff before implementation.

IBM systematically monitors production data center resources 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators to help detect and resolve potential exposures. IBM's data center services support a variety of information

delivery protocols for transmission of data over public networks such as HTTPS, SFTP, and FTPS.

IBM policy defines clear back-up requirements for production systems and data. Compliance with IBM policies is monitored and rigorously enforced. Backup data intended for off-site storage, if any, is encrypted prior to transport.

Security configuration and patch management activities are performed and reviewed regularly. IBM's infrastructure is subject to emergency planning concepts (i.e., disaster recovery, solid disk mirroring, etc.). Business continuity plans for IBM's infrastructure are documented and regularly revalidated.

Activity Logging, Input Control

IBM maintains logs of its activity for systems, applications, and network infrastructure devices. Changes made to production systems are logged and governed in accordance with IBM's strict change management process.

Physical Security, Entry Control

IBM maintains physical security standards designed to restrict unauthorized physical access to data center resources. Only limited access points exist at IBM data centers, which are controlled by access readers and monitored by surveillance cameras. Access is allowed only by authorized personnel.

Delivery areas and loading docks where unauthorized persons may enter the premises are strictly controlled.

Non-IBM operations and security staff are registered upon entering the premises and are escorted by authorized personnel while on the premises.

Employees upon termination are removed from the access list and required to surrender their access badge. Usage of access badges is logged.

Order Control

Data processing is performed only according to our clients' instructions. The instructions are defined in the relevant written agreement by which IBM describes the terms, functionality, support, and maintenance of a SaaS offering and measures taken to ensure the confidentiality, integrity, and availability of client-owned data.

Compliance

IBM security standards are regularly reviewed against broadly accepted, industry standard practices, such as ISO 27001 and SSAE 16 SOC 2. We continue to develop external auditing and certification requirements for IBM SaaS offerings as they and applicable standards and regulations evolve.

Assessments and audits are conducted regularly by IBM to confirm compliance with its information security policies, and industry standard audits are performed annually in all IBM production data centers. A copy of the most recent external audit summary letter is available to clients by written request.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties in order to comply with German Data Privacy Law **(according to sect. 11 subsection 2 BDSG, Federal Data Protection Act, in force since September, 1st 2009 - for reference see http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob =publicationFile):**

Nr.	Specification of	Specified as follows:
1.1	The subject of the work to be carried out:	
1.2	The duration of the work to be carried out:	
2.1	The extent, type and purpose of the intended collection, processing or use of data:	
2.2	The type of data:	
2.3.	The category of data subjects:	
3.	The technical and organizational measures to be taken (for reference see also sect. 9 BDSG):	
4.	The rectification, erasure and blocking of data:	
5.	The processor's obligations under subsection 4 sect. 11 BDSG, in particular monitoring:	The Importer shall
6.	Any right to issue subcontracts:	
7.	The controller's rights to monitor and the processor's corresponding obligations to accept and cooperate:	
8.	Violations by the processor or its employees of provisions to protect personal data or of the terms specified by the controller which are subject to the obligation to notify:	
9.	The extent of the controller's authority to issue instructions to the processor:	
10.	The return of data storage media and the erasure of data recorded by the processor after the work has been carried out:	

Please notes, these are Sample EU Model Clause agreement appendices to be used as a reference for what is in the IBM SaaS EU Model Clause appendices. These are sample documents intended to be used for illustration and are not to be used as part of a transaction. The IBM contracts process will include the official model clause document.