ANNEX II to the Standard Contractual Clauses for transfer (Module 1)

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. Provide details for any measure selected

□ Measures of pseudonymisation and encryption of personal data

(e.g. personal data are stored in an encrypted database. Provide details about the encryption)

□ Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

(e.g. : backup policy, activity logging, drive encryption)

□ Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

(e.g. : existence of a Disaster Recovery Plan or Business Continuity Plan)

□ Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

(e.g. existence of regular external IT security audits)

□ Measures for user identification and authorisation

(e.g. access to resources based on individual login/password, secure password modification policy, policy and procedure for access authorization, use of badges with photo for physical access)

□ Measures for the protection of data during transmission

(e.g. use of https or sftp protocols for secured transmission, use of encrypted emails, portable drives encryption)

□ Measures for the protection of data during storage

(e.g. portable drives encryption, databases encryption at rest)

□ Measures for ensuring physical security of locations at which personal data are processed

(e.g. 24/7 guards, fences, access using badges with photo, fire alarms, fire extinguishers)

□ Measures for ensuring events logging

(e.g. event logging system)

□ Measures for ensuring system configuration, including default configuration

(e.g. Laptop master configuration, management of security patches)

□ Measures for internal IT and IT security governance and management

(e.g. nomination of a Chief Information Security Officer, IT security policy, IT chart)

□ Measures for certification/assurance of processes and products

(e.g. ISO9000, ISO27000 certification)

□ Measures for ensuring data minimisation
(e.g. analysis of personal data processing, erasure of obsolete data, personal data management procedures)

□ Measures for ensuring data quality
(e.g. personal data management procedure, master data management)

□ Measures for ensuring limited data retention
(e.g. personal data lifecycle management process)

□ Measures for ensuring accountability
(e.g. data protection officer nomination, data protection policy including role based processes)

□ Measures for allowing data portability and ensuring erasure
(e.g. data lifecycle policy and procedures)

If technical and organisational measures are described in a separate document, provide details about the Document