ANNEX 1

As specified in the Controller to Controller Data Protection Agreement ("DPA") to which these clauses are appended, the KSA SCCs 2024 MODULE ONE, as published by the Saudi Data & AI authority is incorporated by reference including this Annex which forms an integral part of the KSA SCCs.

Please note that if EU SCCs are already incorporated in the DPA, the information captured in the respective EU SCC Annex shall apply directly to this Annex too. In this case, completion of the current Annex information below is not required.

List of Parties

Information of Personal Data Exporter (s)	Information of Personal Data Importer (s)
Name:	Name:
Address:	Address:
Contact Information:	Contact Information:
Date:	Date:
Role [Controller/Processor]	Role [Controller/Processor]

Description of the Transferred Personal Data

Categories of Personal Data Subjects whose Personal Data is transferred:

Categories of transferred Personal Data:

Categories of transferred sensitive data - if any - and applicable restrictions and safeguards that take full account of the nature of the Personal Data and the risks involved, e.g., purpose limitation, access restrictions, record keeping of access to Personal Data, restrictions on subsequent transfers, or additional organizational, technical, and regulatory measures:

Purpose of Transfer:

Retention Period/Criteria:

Security Measures

The measures below are examples only, and the parties should ensure that the description in this Appendix corresponds to the applicable facts relevant to the transfer.

1-Example: Controlling access to buildings and facilities (physical):

Measures to control access to buildings and facilities, specifically to verify authorization:

- Access control system and card reading system (such as magnetic stripe or chip card).
- Door protection (such as electronic door opening systems and lock sets).
- Security and front desk services.
- Burglar Alarm System (BAS).
- Surveillance Cameras (CCTV).

2-Example: IT system access control (by default):

User identification, access authorization and authentication measures:

- All passwords are electronically authenticated and protected by an encryption system against any unauthorized access attempt or individual or personal user login to access the system and/or corporate networks.
- Additional system logins for specific requests.
- Automatic blocking of the computer after a specified period of time without user activity (as well as password-protected screensavers or activation of the auto-stop function).
- Password procedures (defining acceptable password criteria in terms of difficulty and update intervals).

3-Example: Personal Data access control:

Measures and description of the authorization plan, data access authorizations, and details regarding access control and logging:

- Permit management
- Files
- Roles
- Authorization documentation
- Permit procedures
- Reports/Data logs
- Records of data processing activities

4-Example: Personal Data disclosure control:

Measures to transfer, transmit, or store Personal Data in data media for subsequent verification:

- Email Encryption.
- Secure data networks (e.g., VPN).
- Logging in.
- Protection of media and containers for data storage during physical transportation.
- Secure wireless local area network.
- Secure Port Layer encryption in case of website access.

5-Example: Input Control:

Post-analysis measures whether or not data has been entered, altered, or removed (erased) through:

- Logging and reporting systems.
- Data access rights.
- System logins.
- Security/Login software.

6-Functionality Control:

Measures to separate the responsibilities of the Controller and Processor are as follows:

- A written agreement on the mechanism and system in place for Personal Data Subjects' complaints when their data is processed and describing the rights and obligations of the Controller and Processor.
- Monitoring contractual compliance.
- Train all employees who have access rights and powers to Personal Data.
- Confidentiality and non-disclosure agreements with all relevant employees.
- Conduct regular reviews of Personal Data protection measures.

7-Example: Personal Data accessibility control:

Measures to ensure data availability (physical/virtual):

- Backup procedures.
- Hard disk mirroring.
- Uninterruptible power.
- Keeping backups (e.g., a secure, separate, fireproof partition).
- Activate anti-virus/firewall systems.
- Develop contingency and disaster recovery plans.
- Air conditioners.
- Fire protection systems (including protection from water used for fire suppression).
- Alarm systems.
- Adequate archiving facilities.

8-Example: Personal Data segregation control:

Provide separate Personal Data processing measures (storage, modification, deletion, and transfer) for multiple purposes as follows:

- Separation of development and testing.
- Separation of databases.
- Separation of systems.
- Logical separation between different customer databases