

KSA – Standard Contractual Clauses

(Controller to Controller)

Clause (1) Purpose and Scope

A. The purpose of these Clauses is to ensure that an appropriate level of Personal Data protection equivalent to the level of protection applicable under the Personal Data Protection Law and its Implementing Regulations is applied in the absence of an appropriate level of Personal Data protection outside the Kingdom by specifying the obligations of the parties involved in the transfer of Personal Data to a country or international organization that does not have an appropriate level of Personal Data protection. Appendix (1) shows the data for both Data Exporters and Data Importers.

B. These Clauses apply to the transfer of Personal Data as specified in Appendix (2) ("Personal Data to be Transferred or Disclosed").

Clause (2) Impact and Modification

A. These Clauses set out appropriate safeguards, including rights of complaint by Personal Data Subjects, and cannot be amended except to select the appropriate template or to add or update information in the appendix.

B. The parties may incorporate these Clauses into a comprehensive agreement or add other clauses or additional guarantees, provided they do not directly or indirectly conflict with these Clauses or infringe on the fundamental rights of Personal Data Subjects.

C. These Clauses do not relieve any party from its obligations under the Law and Regulations, nor do they prejudice the provisions of the Laws and Regulations in force in the Kingdom or agreements to which the Kingdom is a party.

Clause (3) Rights of Personal Data Subjects

A. These Standard Contractual Clauses are without prejudice to the rights of Personal Data Subjects under the Law and Regulations.

B. Personal Data Subjects whose Personal Data is transferred from the parties based on these Standard Contractual Clauses may notify the Competent Authority ("Saudi Data & AI Authority") if they become aware of any violation of these Standard Contractual Clauses.

Clause (4) Interpretation

A. Unless the context requires otherwise, the words and phrases used in these Clauses shall have the meanings assigned to them in Article (1) of the Personal Data Protection Law issued by Royal Decree No. (M/19) dated 9/2/1443 AH and amended by Royal Decree No. (M/148) dated 5/9/1444 AH, Article (1) of the Implementing Regulation of the PDPL and Article (1) of the Regulation on the Transfer of Personal Data Outside the Kingdom.

B. These Clauses must be read and interpreted in light of and in accordance with the provisions of the Law and Regulations referred to in paragraph (a) of this Article, and may not be interpreted in any other way that is inconsistent with the provisions of the Law and Regulations.

Clause (5) Conflict

In the event of a conflict between these Clauses and any provision in any other agreement between the parties, these Clauses shall prevail.

Clause (6) Details of Transfers

The transfer(s), as well as the categories of Personal Data and the purposes of the transfers, are described in the Appendix.

Clause (7) Addition of New Parties

A. Any Personal Data Importer or Personal Data Exporter who is not a party to these Standard Clauses may join these Standard Contractual Clauses by completing and signing Appendix (1), with the consent of the existing parties. The Joining Entity shall be either the Personal Data Importer or the Personal Data Exporter.

B. Once Appendix (1) has been completed and signed, the Joining Entity shall be a party to these Clauses, and the newly Joined Entity shall, as of the date of joining, and assume the responsibilities depending on the nature of the Personal Data processing and transfer operations that occurred on or after the date of joining, and shall be entitled to exercise the rights and obligations corresponding to its role as defined in these Clauses.

Clause (8) Governing Law and Jurisdiction

These Standard Contractual Clauses shall be governed by the applicable laws of the Kingdom of Saudi Arabia. Any dispute arising from the application of the provisions of these Clauses shall fall under the jurisdiction of the Kingdom and be vested in its courts. The Personal Data Importer, under these Standard Contractual Clauses, agrees to submit to the jurisdiction of the Kingdom of Saudi Arabia.

Clause (9) Compliance with the Requests of the Competent Authority

A. Each party agrees to comply with any requests from the Competent Authority in relation to these Standard Contractual Clauses or the processing of transferred Personal Data.

B. The Personal Data Importer agrees and commits to cooperate with the Competent Authority and comply with all its requests and inquiries and provide the necessary documents and information to ensure compliance with the Standard Contractual Clauses.

C. The Personal Data Importer agrees to abide by the measures adopted by the Competent Authority, including corrective measures and compensation.

Clause (10) Compensation

A. If any dispute arises between the Personal Data Subject and a party regarding compliance with the Standard Contractual Clauses, that party shall use all necessary means to settle the

dispute amicably with the Personal Data Subject, and all parties shall inform each other of the existence of such dispute to ensure that it is resolved in cooperation with each other.

B. The Personal Data Subject may submit to the Competent Authority any complaint arising from the application of the provisions of these Standard Contractual Clauses, in accordance with the procedures for submitting complaints specified by the Law and Regulations.

C. The Personal Data Subject has the right to claim before the competent court for compensation for material or moral damage in proportion to the magnitude of the damage arising from the application of these Standard Contractual Clauses.

Clause (11) Personal Data Security

A. All parties shall take the necessary organizational, administrative, and technical measures that ensure to maintain the privacy of personal Data against any breach at all stages of processing, including personal data security during the transfer process. In assessing the appropriate level of security, the Parties shall take into account the current state of technology, implementation costs, and the nature of the Personal Data transferred, as well as the nature, scope, context, purposes, the risks involved in the processing of the Personal Data, and specifically consider the application of encryption or de-identification, including during Personal Data transfer, where the purpose of the data processing can be achieved in this way.

B. The Personal Data Exporter shall assist the Personal Data Importer in fulfilling the necessary data security requirements, and in the event of any Personal Data breach in relation to the transferred Personal Data processed by The Personal Data Exporter under these Standard Contractual Clauses, The Personal Data Exporter shall notify the Personal Data Importer without delay after becoming aware of such breach and shall assist the Personal Data Importer in containing such breach.

C. The Data Exporter ensures that persons authorized to process the transferred Personal Data are bound by confidentiality and non-disclosure under an appropriate legal obligation of confidentiality and non-disclosure.

Clause (12) Duration and Termination

A. If, for any reason, the personal Data Importer is unable to fulfill its obligations under these Standard Contractual Clauses, it must inform The Personal Data Exporter within (24) hours from the time it becomes aware of this.

B. In the event that the personal Data Importer violates these Standard Contractual Clauses or is unable to comply with them, the personal Data Exporter shall immediately cease the transfer of Personal Data to the Personal Data Importer until the Personal Data Importer ensures its return to compliance again, provided that the Personal Data Importer shall be given a period of (30) days, extendable for a similar maximum period, to prove its ability to comply with these Clauses, and if the period expires without achieving this, the two parties shall agree to terminate the contract, without any liability for the Personal Data Exporter or Controller, as the case may be.

C. The Personal Data Exporter or Controller, as the case may be, shall ensure that all Personal Data previously transferred to the Personal Data Importer is fully destroyed before terminating the Standard Contractual Clauses under paragraph (b) above. It shall also ensure that any copies it has of such personal data are destroyed.

D. The Personal Data Importer must document the destruction of the data, and this documentation must be provided to the Personal Data Exporter or controller upon request.

E. The Personal Data Importer must continue to ensure - until the data is destroyed - that it complies with these Standard Contractual Clauses.

Clause (13) Protection of Transferred Personal Data

The Personal Data Exporter and the Personal Data Importer shall process the transferred Personal Data according to the nature and purposes of the transfer and the appropriate template as follows:

First Template: Controller to Controller

1. Processing Restrictions

The personal Data Importer is obliged to process the transferred Personal Data in accordance with the purposes set out in Appendix (2).

2. Compliance with the Requests of the Competent Authority

A. The parties shall provide a copy of these Clauses to the Competent Authority upon request and without undue delay in order for the Competent Authority to exercise its powers under the Law and Regulations. The Competent Authority may request any additional information regarding the transfers of Personal Data.

B. Each party agrees to comply with any requests made by the Competent Authority in relation to these Clauses or the processing of the transferred data.

C. Upon request, the Personal Data Importer (either directly or through The Personal Data Exporter) shall disclose its identity and contact details and the categories of Personal Data being processed to the Personal Data Subject and provide a copy of these items.

3. The Minimum Amount of Personal Data Needed to Fulfill the Purpose

All parties shall ensure that the Personal Data transferred is sufficient and limited to the minimum amount necessary to fulfill the purposes set out in Appendix (2). If any party becomes aware of any transfer of unnecessary Personal Data, that party shall inform the other party(ies) as soon as it becomes aware of it.

4. Personal Data Retention

The Personal Data Importer shall retain the transferred Personal Data if it is necessary to fulfill the purposes set out in Appendix (2), provided that the Personal Data Importer shall, without undue delay, delete or anonymize the transferred Personal Data except in the following cases:

A. If it is in accordance with a legal justification under the Kingdom's laws and the Personal Data Protection Law and its Regulations; in this case, the data shall be destroyed after expiration of the period or once the purpose for collecting it has been fulfilled, whichever is longer.

B. If retaining the transferred personal data for an additional period is directly related to a case pending before a judicial authority, and such retention is required for this purpose, the data shall be destroyed after completion of the judicial procedures related to the case.

C. If retaining the transferred personal data for an additional period is necessary to protect the life of the data subject or their vital interests.

5. Personal Data Security and Personal Data Breach Incident Notifications

The Parties shall ensure that the organizational, administrative, and technical measures specified in Appendix (3) provide a sufficient level of protection for the transferred Personal Data to comply with the requirements of Article (19) of the Law and Article (23) of the Implementing Regulations.

A. The Personal Data Importer shall implement the security measures specified in Appendix (3) and apply those measures to all Personal Data transferred to ensure the security and protection of Personal Data against any violation that may result in damage to the Personal Data Subject, unlawful action, loss, alteration, disclosure of Personal Data or unauthorized access.

B. The Personal Data Importer must periodically review the security measures stipulated in Appendix (3) to ensure that they are being implemented as required, and update them as needed to ensure compliance with Article (19) of the Law and Article (23) of the Implementing Regulations. If the Personal Data Importer becomes aware of a data breach incident that could harm the transferred personal data or the data subjects, or conflict with their rights or interests, the Personal Data Importer must notify the competent authority within (72) hours of becoming aware of the incident, in accordance with the requirements stated in Article (24) of the Implementing Regulations of the Law.

6. Sensitive Data

Without prejudice to any restrictions relating to sensitive data stipulated in the Law and the Implementing Regulations of the Law, the Personal Data Exporter shall ensure that the Personal Data Importer adopts additional safeguards appropriate to the nature of the sensitive data and ensures that it is protected from any risks when processing it while ensuring that the restrictions and additional safeguards described in Appendix (2) are applied.

7. Subsequent Transfer

A. The Personal Data Importer shall not transfer or disclose the transferred Personal Data to a third party outside the Kingdom unless that party has acceded to these Clauses and in accordance with the appropriate template and the provisions of Clause (7) above.

B. Without prejudice to the provisions of Articles (8) and (15) of the Law and (17) of the Implementing Regulation of the Law, the provisions of the Law and Regulations shall apply to subsequent transfer of Personal Data that has been previously transferred or disclosed to an entity outside the Kingdom.

8. Assigning Processors

The Personal Data Importer shall be obliged to select a Processor that provides sufficient guarantees for the protection of the transferred Personal Data, and the agreement with the Processor shall include all the requirements set out in Article (17) of the Implementing Regulation, and the processing shall be based solely on the instructions of the Data Importer, provided that these instructions are consistent with the requirements set out in these Clauses.

9. Compliance with these Clauses

A. All parties shall demonstrate full compliance with these Clauses to the Competent Authority upon request, and the Personal Data Importer shall maintain documents related to the Personal Data processing activities conducted under its supervision, in addition to the records of Personal Data processing activities as stipulated in Article (33) of the Regulation.

B. The Personal Data Importer shall provide these documents to the Competent Authority upon request.

10.Accountability

A. Each party shall be accountable to the other party for any damages caused to the other party as a result of a breach of any of these Standard Contractual Clauses.

B. Each party shall be accountable to the Personal Data Subject, without prejudice to the accountability of the Personal Data Exporter under the Law and Regulations, and the Personal Data Subject shall be entitled to compensation for any material and moral damages caused by the negligent party that harms the Personal Data Subject. If more than one party is responsible for causing damage to the Personal Data Subject as a result of the violation of these Standard Contractual Clauses, the responsible parties shall be held jointly or individually accountable, and the Personal Data Subject shall have the right to take legal action before a court against any of these parties.

C. The parties agree that if any party assumes accountability (b), it shall be entitled to claim from the other party(ies) that portion of the compensation corresponding to his/her/their accountability for the damage.

D. The Personal Data Importer may not rely on the behavior of the data Processor or Sub-Processor to avoid accountability.

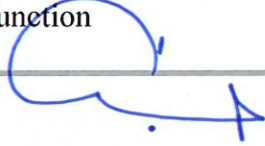
11.Right of Personal Data Subjects

A. The Personal Data Importer (with the support of the Personal Data Exporter) shall deal, as appropriate, with any queries or requests received from the Data Subject regarding the processing of Personal Data and the exercise of the rights provided for in accordance with the Law and applicable regulations without any delay within a period of no more than thirty (30) days from the date of receipt of such request. This period may be extended for a similar period up to a maximum of thirty (30) days if the execution of the request requires extraordinary effort or if the Personal Data Importer receives many requests from the Personal Data Subject. The Data Subject is notified in advance of this extension and its reasons.

B. All statements made to the Personal Data Subject must be presented in a clear, legible, and accessible format.

Appendix 1 - Parties of List

[Note: The data in this appendix is updated for all phases]

Information of Personal Data Exporter (s)	Information of Personal Data Importer (s)
Name: As stated in our terms of engagement (known as 'the KSA Client' in this SCC Agreement)	Name: As stated in our terms of engagement (known as 'Clyde & Co' in this SCC Agreement)
Address: As stated in our terms of engagement	Address: As stated in our terms of engagement
Contact Information: Please contact the KSA Client for contact details of the KSA Client's data compliance function	Contact Information: Please contact Clyde & Co for contact details of Clyde & Co's data compliance function
Signature:	Signature: 
Date:	Date: 21.7.2025
Role: Controller	Role: Controller

Appendix 2 - Description of the Transferred Personal Data

[Note: The data in this appendix is updated for all Phases]

Categories of Personal Data Subjects whose Personal Data is transferred

The personal data transferred under the KSA Client to Clyde & Co International Data Transfer will concern one or more of the following categories of data subjects:

- individuals that work for, own or represent the KSA Client;
- individuals that work for, own or represent the KSA Client's service providers;
- individuals that are either directly or indirectly involved or connected with, or relevant to, a matter on which Clyde & Co is advising the KSA Client (either directly or indirectly); and
- individuals whose details are transferred to Clyde & Co in connection with our role as the legal representative of the KSA Client

Categories of transferred Personal Data

The KSA Client to Clyde & Co International Data Transfer will include the transfer of one or more of the following categories of personal data:

- individual details – name, address (including proof of address), other contact details (e.g. email and telephone numbers), gender, marital status, date and place of birth, nationality, employer, job title and employment history, and family details, including their relationship to the data subject;
 - identification details – identification numbers relating to the data subject issued by government bodies or agencies, such as Iqama numbers, passport numbers, and driving licence numbers;
 - financial information – bank account or payment card details, income or other financial information about the data subject;
 - matter details – information about the data subject which is relevant to a matter on which Clyde & Co is advising the KSA Client;
 - credit, anti-fraud and sanctions data – credit history, credit score and information received from various anti-fraud and sanctions databases relating to the data subject; and
 - identifiers – information which can be traced back to the data subject, such as an IP address, a website tracking code or electronic images of the data subject.
-
-

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

Where relevant, the KSA Client to Clyde & Co International Data Transfer may include the transfer of the following categories of sensitive data:

Sensitive data: information about racial or ethnic origin, religious, intellectual or political belief, biometric or genetic data for the purpose of identifying the person, health data and data that indicates that one or both of the individual's parents are unknown, in each case where relevant to the purposes of the transfer.

Criminal convictions data: information relating to security criminal convictions and offences.

Please contact the data importer for further details about restrictions and safeguards in place for the sensitive data transferred.

Purpose of Transfer

The KSA Client to Clyde & Co International Data Transfer is made for one or more of the following main purposes:

- to provide the KSA Client with legal advice and related services;
- to carry out relevant credit checks;
- to manage and develop Clyde & Co's business with the KSA Client, which may include using the personal data for marketing purposes where relevant; and
- to comply with the Clyde & Co Entity's, and the wider Clyde & Co group's, legal and regulatory requirements.

Full details of the purposes for which the Clyde & Co Entity may use the personal data are set out in the Clyde & Co privacy notice, a copy of which can be found at www.clydeco.com/help/privacy.

Retention Period/Criteria:

The personal data will be retained by the data importer in accordance with its global data retention policy which categorises all of the information held by it and specifies the appropriate retention period for each category of information. Those periods are based on the requirements of relevant data protection laws and the purpose for which the information is collected and used, taking into account legal and regulatory requirements to

retain the information for a minimum period, limitation periods for taking legal action, good practice and our business purposes.

Appendix 3 - Security Measures

[Note: The data in this appendix is updated for all Phases]

1. All parties are obliged to clarify the organizational, administrative, technical, and security measures that will be applied to the transferred Personal Data to fulfill the provisions of Article (19) of the Law and Article (23) of the Implementing Regulation of the Law.
2. 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 Controlling access to buildings and facilities (physical):

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

- Token controlled access gates
- Manned entry/exit points.
- Surveillance Cameras (CCTV).
- Coded locks on doors and alarms.
- Access control and logging systems installed on doors leading to office areas.
- Visitor log.

2 IT system access control (by default):

User identification, access authorization and authentication measures:

- We use active directory to identify and authorise users to access our systems and infrastructure.
- As part of our authorisation processes, remote users also authenticate using multi-factor authentication. We schedule qualified external penetration testers on an annual basis and also carry out penetration testing on suppliers where this is appropriate.
- Clyde & Co implement the principal of least privilege to all access methods.

3 Personal Data access control:

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

- Clyde & Co implement industry best practice, manufacturer guidelines and standards to implement robust secure configurations.
- Clyde & Co ensures that all authentication and access activity is logged to a SIEM and monitored 24/7.
- Records of data processing activities.

4 Personal Data disclosure control:

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

- We have opportunistic TLS Encryption in transit in place.
- We have information security policies and procedures based on industry best practice and international standards, in order to ensure the security of our systems. Email Encryption.
- Clyde & Co ensures that data is encrypted at rest using industry standard algorithms.
- Clyde & Co ensures that encryption keys are managed by the firm and that such keys are changed regularly.

5 Input Control:

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

- We have a security information and event measurement system which collects and analyses event logs in order to identify exceptional events (e.g brute force attacks) and allow the appropriate action to be taken.
- Clyde & Co implement individual user accounts, strong passwords and Multi-factor authentication together with appropriate conditional access policies, to control all access to resources and data.

6 Functionality Control:

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

- We assess the security posture of suppliers using a risk based assessment procedure.

-
- 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.

Other controls are as follows:

- Clyde & Co LLP is our UK headquarters which maintains both Cyber Essentials Plus and ISO27001:2022 certification. This involves us submitting to regular external assessments.
- Clyde & Co implement information security risk management processes and operates a risk register to ensure that recognised risks are appropriately mitigated.

Personal Data accessibility control:

Measures to ensure data availability (physical/virtual):

- Clyde & Co maintains disaster recovery and business continuity plans that are reviewed and tested periodically.
- Clyde & Co implement resilient infrastructure with multiple availability zones where possible.
- Clyde & Co implement a backup strategy for data and ensure that backups are encrypted, then secured remotely from the backup site.
- Clyde & Co implement appropriate environmental controls in all of its data processing facilities including that of their supply chain.
- Clyde & Co utilise next generation anti-virus/malware and EDR software on all endpoints to protect against online threats.
- Archiving facilities.

Personal Data segregation control:

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

- Clyde & Co provides a logical marking of data within databases to provide adequate segmentation.
- Clyde & Co ensure that singular systems are not used to run more than one service or database.
- Clyde & Co ensures that development, testing and production environments remain separated. Additional controls exist to prevent developer access to production code or data.
- Clyde & Co implements a Change Control process to manage all change.

Please contact the data importer for further details.