



SDAIA

الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority

Standard Contractual Clauses For --- Personal Data Transfer

Document Classification: **Public**

Version 1.0

September 2024



Table of Contents

| | |
|--|----|
| Introduction..... | 4 |
| Purpose | 4 |
| Definitions | 4 |
| Scope..... | 6 |
| Standard Contractual Clauses Rules | 6 |
| Standard Contractual Clauses Templates | 8 |
| Appendices | 9 |
| Appendix 1 - Parties of List | 35 |
| Appendix 2 - Description of the Transferred Personal Data..... | 36 |
| Appendix 3 - Security Measures..... | 37 |

Introduction

Based on the Personal Data Protection Law, issued by Royal Decree No. (M/19) dated 9/2/1443 AH (the "Law") and amended by Royal Decree No. (M/148) dated 5/9/1444 AH, and its contents on the permissibility of transferring Personal Data outside the Kingdom. The Regulation on the Transfer of Personal Data Outside the Kingdom ("Transfer Regulation") sets out the provisions to be followed upon transfer, including the Clauses applied in cases where Controllers are exempted from the requirements to comply with the level of protection and the minimum level of transfer of Personal Data stipulated in subparagraphs (B) and (C) of paragraph (2) of Article (29) of the Law and provisions of the Regulation on the Transfer of Personal Data Outside the Kingdom.

Purpose

The purpose of these Clauses is to ensure the application of a level of protection of Personal Data equivalent to the level of protection applied under the Law and Regulations 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. These Clauses are one of the appropriate safeguards that Controllers and Processors may use in addition to the Binding Common Rules (BCR) and accreditation certificates from a body licensed by the Competent Authority.

Definitions

In this document, unless explicitly stated otherwise, the following terms shall have the meanings assigned to each of them below:

The Kingdom: The Kingdom of Saudi Arabia (KSA)

The Law: The Personal Data Protection Law (PDPL) 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.

Regulations: The Implementing Regulations of the Law “Includes both of the implementing Regulations and the implementing Regulation for Personal Data Transfer outside the Kingdom.”

The Competent Authority: Saudi Data & AI Authority (SDAIA)

Appropriate Safeguards: The requirements imposed by the competent authority on controllers, which include adherence to the Law and Regulations when transferring or disclosing personal data to entities outside the Kingdom. This applies in cases where exemptions are granted from the conditions for providing an appropriate or minimum level of personal data protection, to ensure appropriate level of protection when transferring personal data outside the Kingdom that meets at least the standards prescribed by the Law and Regulations.

Standard Contractual Clauses: Mandatory provisions governing the transfer of personal data outside the Kingdom that ensure appropriate level of protection for such data not less than the standard prescribed by the Law and Regulations. These provisions are in accordance with a standard form issued by the competent authority.

International Organization: A legal body comprising members from at least three countries, operating in multiple sovereign states, established through a formal legal document such as a treaty or agreement based on international law, and this legal document defines the aims and objectives of the international organization and its structures, decision-making powers and

jurisdiction. (e.g. the United Nations, the World Bank, the League of Arab States, the Arab Monetary Fund). These organizations engage in international activities and must comply with various Personal Data protection laws across different jurisdictions.

Transfer of Personal Data: Transfer, disclosure (or granting of access) of Personal Data from the Kingdom of Saudi Arabia to Controllers, Processors, or other recipients in countries or international organizations other than the Kingdom of Saudi Arabia where neither the Personal Data Exporter nor the Importer of the Personal Data.

Third-Party Data Transfers/Subsequent Transfers: The transfer of Personal Data from an external country or international organization to Controllers or Processors within the same country/organization or in another country/organization.

Scope

This document specifies the Standard Contractual Clauses issued by the Competent Authority in Appendix (1) of this document. These Clauses also apply to data controllers or Processors based on the instructions of the data controller and on their behalf, without prejudicing the responsibilities of the data controller to the competent authority or the data subject, as applicable, when transferring Personal Data outside the Kingdom to a country or international organization that does not have an appropriate level of Personal Data protection.

Standard Contractual Clauses Rules

1. The Standard Contractual Clauses, as set out in Appendix (1) attached to this document, provide protection for Personal Data and an appropriate guarantee

in accordance with the provisions of the Law and Regulations for the transfer or disclosure of Personal Data to entities outside the Kingdom from the Personal Data Exporter to the Personal Data Importer.

2. Standard Contractual Clauses specify Clauses that must be included in a contract or agreement between the Personal Data Exporter and the Personal Data Importer or placed in a separate contract or agreement.
3. The adoption of Standard Contractual Clauses does not prejudice the parties' obligations under the Law and Regulations when processing Personal Data.
4. If the Standard Contractual Clauses are included in a contract or agreement, no explicit or implicit term or provision therein shall conflict with them or limit the scope of their application or the protection expected from them. In addition, the contracting parties have the right to include any additional conditions related to the processing of Personal Data, provided that such additional conditions do not contradict and/or undermine any of the requirements of the Standard Contractual Clauses or the Law and Regulations.
5. If any party modifies the approved text (except the blank fields that are required to be filled in Standard Contractual Clauses), such modifications shall not be recognized by the Competent Authority and shall be deemed a violation of the provisions of the Law and Regulations.
6. Standard Contractual Clauses can involve more than two parties, so Controllers and additional Processors can join these Clauses as Personal Data Exporters or Personal Data Importers, depending on the nature of their role throughout the duration of the contract.
7. Personal data may not be transferred under the Standard Contractual Clauses if the laws and regulations of the recipient country or international organization

prevent the Personal Data Importer from complying with the Standard Contractual Clauses.

8. To ensure effective enforcement of these Clauses, the Personal Data Importer submits to the jurisdiction of the Kingdom and undertakes to comply with and enforce any binding decision under applicable Kingdom Laws and Regulations.
9. The Personal Data Importer must agree to respond to the Competent Authority's requests and cooperate with its auditing procedures and approved compliance follow-up measures, including corrective measures and actions, and confirm to the Competent Authority in writing that the necessary actions have been taken.
10. After the adoption of the Standard Contractual Clauses, if the Personal Data Exporter determines that the Personal Data Importer is unable or no longer able to fulfill the obligations set forth in these Clauses, or the Personal Data Importer notifies the Personal Data Exporter if there is reason to believe that the obligations set forth in these Clauses cannot be fulfilled, the Personal Data Exporter must suspend transfers unless alternative measures or guarantees are adopted that meet the requirements set forth in the Law and Regulations.
11. The Competent Authority may, at its discretion, make any change to the Standard Contractual Clauses contained in this document, and if any change is made, the Competent Authority will issue rules regarding transitional measures, as well as rules regarding the remaining validity period of agreements under the previous Standard Contractual Clauses.

Standard Contractual Clauses Templates

The Standard Contractual Clauses templates have been prepared to include general Clauses that apply to all contractual situations, as well as other Clauses of a specific nature according to the roles of the parties involved. Before

implementing the Standard Contractual Clauses, all parties must identify the template that applies to the relevant transfers according to the nature of their roles and delete those that do not apply:

First Template: Controller to Controller: This template applies to transfers of Personal Data outside the Kingdom from one Controller (the Personal Data Exporter) to another Controller (the Personal Data Importer).

Second Template: Controller to Processor: This template applies to transfers of Personal Data outside the Kingdom from a Controller (the Personal Data Exporter) to a Processor (the Personal Data Importer).

Third Template: Processor to Processor: This template applies to transfers of Personal Data outside the Kingdom from a Processor (the Personal Data Exporter) to a Sub-Processor (the Personal Data Importer).

Fourth Template: Processor to Controller: This template applies to transfers of Personal Data outside the Kingdom from a Processor (the Personal Data Exporter) to a Controller (the Personal Data Importer).

Appendices

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.

Conflict (5) Clause

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.

Second Template: Controller to Processor

1.Processing Instructions

The Personal Data Importer shall only process the transferred Personal Data based on written instructions from the Personal Data Exporter. Accordingly, if the Personal Data Importer is unable to follow the instructions, it shall inform the Personal Data Exporter in writing without undue delay.

2.Processing Restrictions

The Personal Data Importer shall process the transferred Personal Data in accordance with the purposes specified in Appendix (2), unless otherwise directed in writing by the Personal Data Exporter, provided that the Personal Data shall be processed in accordance with the provisions of the Law and its Implementing Regulations in all cases.

3.Compliance with the Requests of the Competent Authority

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

4.Accuracy and Quality of Personal Data

If The Personal Data Importer realizes that any Personal Data transferred is inaccurate or not up-to-date, it shall inform the Personal Data Exporter in writing without undue delay, in which case the Personal Data Importer shall destroy the Personal Data and notify the Personal Data Exporter accordingly, unless the Personal Data Exporter is instructed not to destroy the data because it wishes to correct the transferred Personal Data.

5.Duration of Personal Data Processing and Destruction or Recovery

- A. The processing shall be carried out by the Personal Data Importer only for the period specified in Appendix (2). After completion of the purpose of the processing, The Personal Data Importer shall destroy all Personal Data processed on behalf of the Personal Data Exporter and notify the Personal Data Exporter accordingly unless otherwise instructed by the Personal Data Exporter in the following cases:
 - 1. Return all processed Personal Data to the Personal Data Exporter and delete the copies held by the Data Importer;
 - 2. If the applicable regulations in the Kingdom require the retention of the transferred Personal Data for an additional period of time;

B. The Personal Data Importer remains bound by these Clauses until the Personal Data is deleted or recovered.

6. Personal Data Security and Personal Data Breach Notifications

A. 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 Regulation.

B. The Personal Data Importer shall implement the security measures specified in Appendix (3) and apply those measures to all transferred Personal Data 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, or unauthorized access to Personal Data.

C. The Personal Data Importer must periodically review the security measures stipulated in Appendix (3) to ensure that they are implemented as required and update them as needed to ensure compliance with Article (19) of the Law and Article (23) of the Implementing Regulation.

D. If The Personal Data Importer becomes aware of a Personal Data Breach incident that affects the transferred Personal Data or is likely to cause damage to the rights and interests of Personal Data Subjects, the Personal Data Importer must immediately take appropriate and necessary measures to contain the incident to minimize any risks or negative consequences and ensure that it is prevented from reoccurring. The Personal Data Exporter must be notified within (24) hours from the time of occurrence or knowledge of the breach incident, provided that the notification includes a description of the incident, its causes, the measures taken or planned to be taken to

contain the incident and prevent its reoccurrence, in addition to the contact details for follow-up by the Personal Data Exporter. If the Personal Data Exporter realizes that the incident may cause damage to Personal Data or Personal Data Subjects or contradict their rights or interests, it shall notify the Competent Authority within (48) hours and in accordance with the requirements set out in Article (24) of the Law's Implementing Regulation.

- E. As soon as the Personal Data Exporter receives the Data Importer's notification of a Personal Data breach incident and the incident would harm the Personal Data or the Personal Data Subject or contradict his/her rights or interests, the Personal Data Exporter must provide immediate notification in simple and clear language in accordance with the provisions of Article (24) of the Implementing Regulation to the Personal Data Subjects affected by the data breach incident, provided that the notification includes the potential risks and their nature, the measures taken or planned to be taken to contain the incident, and the contact information of the Personal Data Exporter, Data Importer, and the respective Personal Data Protection Officer of both entities, along with recommendations or consultations to aid the Data Subject in preventing or minimizing the impact of the outlined risks.

7.Sensitive Data

Without prejudice to any restrictions related 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 means of protection commensurate with the nature of the sensitive data and guarantees its protection from any risks when processing it, while ensuring that the restrictions and additional guarantees described in Appendix (2) are applied.

8. 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 Personal Data that has been previously transferred or disclosed to an entity outside the Kingdom.

9. Compliance with these Clauses

- A. The Personal Data Importer shall respond to all inquiries of the Personal Data Exporter within the specified period and provide all information requested by the Personal Data Exporter, in addition to providing the Personal Data Exporter with all information it may request regarding the processing of the transferred Personal Data, including any information necessary to enable the Personal Data Exporter to prove its compliance with the requirements contained in these Clauses or the provisions stipulated in the Law and its Implementing Regulations.
- B. Each party shall be responsible for demonstrating to the Competent Authority, upon request, that all obligations under these Clauses have been fulfilled.
- C. The Personal Data Importer allows the Personal Data Exporter or its appointed representatives to audit the Data Importer's processing of Personal Data without undue delay upon Personal Data Exporter's request.
- D. The Personal Data Exporter must provide the information revealed by the audit when requested by the Competent Authority.

E. The right of audit does not grant the Personal Data Exporter or its representatives access to any confidential information of the Personal Data Importer as long as this information is not closely related to the processing of the transferred Personal Data.

10. Rights of Personal Data Subjects

A. The Personal Data Importer shall notify the Personal Data Exporter within (48) hours from the time of receipt of the request of any request received from the Personal Data Subject, and the Personal Data Importer shall not have the right to respond to such requests unless the Personal Data Exporter authorizes it to do so.

B. The Personal Data Importer shall take all necessary measures in cooperation with the Personal Data Exporter to respond to the requests of Personal Data Subjects and enable them to exercise their rights under the provisions of the Law and Regulations.

C. The Personal Data Importer is obligated to follow all instructions issued by the Personal Data Exporter regarding the processing of the transferred Personal Data.

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

Third Template: Processor to Processor

1. Instructions Processing.

A. The Personal Data Exporter has clarified to the Personal Data Importer that it processes Personal Data as a Processor based on the instructions of, and on behalf of, its Controller. The Personal Data Exporter confirms that these instructions are compatible and consistent with the instructions provided to it by the Controller.

- B. The Personal Data Importer is obliged to process the transferred Personal Data only upon written instructions from the Personal Data Exporter. The Personal Data Importer is obliged to inform the Personal Data Exporter if it is unable to follow these instructions without undue delay.
- C. The Personal Data Importer shall notify the Personal Data Exporter if it is unable to comply with The Personal Data Exporter's instructions within (24) hours from the time it becomes aware of this, provided that the Personal Data Exporter shall notify the Controller within (48) hours from the time it receives the Data Importer's notification.
- D. The Personal Data Exporter confirms that it has imposed obligations on the Personal Data Importer equivalent to those imposed on the Personal Data Exporter by the Controller with respect to the processing of transferred Personal Data.

2. Processing Restrictions

The Personal Data Importer shall process the transferred Personal Data in accordance with the purposes specified in Appendix (2), unless otherwise directed in writing by the Personal Data Exporter, provided that the Personal Data shall be processed in accordance with the provisions of the Law and its Implementing Regulations in all cases.

3. Compliance with the Requests of the Competent Authority

- A. In order for the Competent Authority to exercise its powers under the Law and the Implementing Regulations, the parties shall provide a copy of these Clauses to the Competent Authority upon request and without undue delay. The Competent Authority may request any additional information regarding 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 or the Controller) shall disclose its identity, contact information, and the categories of Personal Data being processed to the Personal Data Subject and provide a copy of these Clauses.

4. Accuracy and Quality of Personal Data

If The Personal Data Importer realizes that any transferred Personal Data is inaccurate or not up-to-date, it shall inform the Personal Data Exporter in writing without undue delay, provided that the Personal Data Exporter shall inform the Controller within (48) hours from the time the Personal Data Importer notifies the Personal Data Exporter to request a written directive requesting the destruction or correction of the Personal Data.

5. Duration of Personal Data Processing and Destruction or Recovery

- A. The processing shall be carried out by the Personal Data Importer only for the period specified in Appendix (2). After completion of the purpose of the processing, the Personal Data Importer shall destroy all Personal Data processed on behalf of the Personal Data Exporter and notify the Personal Data Exporter accordingly, unless otherwise directed by the Personal Data Exporter in the following cases:
 - 1. Return all processed Personal Data to the Personal Data Exporter and delete the copies held by the Data Importer;
 - 2. If the regulations in force in the Kingdom require the retention of the transferred Personal Data for an additional period of time;

3. To retain the minimum amount of Personal Data necessary for the establishment, prosecution, or defense of legal proceedings;

4. Retain the minimum amount of transferred Personal Data necessary to protect the Data Subject's life or vital interests or to prevent, examine, or treat an infection.

b. The Personal Data Importer remains bound by these Clauses until the Personal Data is deleted or recovered.

6. Personal Data Security and Personal Data Breach Notifications

A. 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 Regulation.

B. The Personal Data Importer shall implement the security measures specified in Appendix (3) and apply those measures to all transferred Personal Data 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, or unauthorized access.

C. 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 Regulation.

If 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 immediately take appropriate and necessary measures to contain the incident to minimize any risks or negative consequences and ensure that it does not recur. The Personal

Data Exporter must be notified within 24 hours of the breach or upon becoming aware of it. This notification shall include a description of the incident, its causes, the measures taken or planned to contain the incident and prevent its recurrence, and contact details for follow-up by the Personal Data Exporter. The Personal Data Exporter must notify the controller within 24 hours of receiving the notification from the Data Importer. The controller must then notify the competent authority in accordance with the requirements set forth in "Article 24" of the Implementing Regulations of the Law.

7. Sensitive Data

Without prejudice to any restrictions related to sensitive data as stipulated in the Law and its Implementing Regulations, the Personal Data Exporter must ensure that the Data Exporter adopts additional protection measures appropriate to the nature of the sensitive data and ensures its protection from any risks during processing, while also ensuring the application of the restrictions and additional safeguards outlined in Appendix (2).

8. Subsequent Transfer

- A. The 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 Personal Data that has been previously transferred or disclosed to an entity outside the Kingdom.
- C. The Controller shall be responsible for verifying that the Personal Data Exporter and Data Importer comply with the above obligations, and the

Controller may appoint an independent third party to review and verify compliance on its behalf. In all cases, if the Personal Data Exporter and Data Importer violate the instructions issued by the Controller or the agreement concluded with it regarding the processing of the transferred Personal Data, the Personal Data Exporter and Data Importer shall be considered as the Controller and shall be responsible for violating the Standard Contractual Clauses and the provisions of the Law and the Implementing Regulations before the Competent Authority.

9. Sub-Processor Appointment

- A. If there is a need for the Personal Data Importer to appoint a Sub-Processor, the Personal Data Exporter is required to obtain prior written consent from the Controller at least [specify time period] before appointing any Sub-Processor.
- B. If a Sub-Processor is appointed, this shall be done through a written agreement that imposes the same obligations as on the Personal Data Importer under these Standard Contractual Clauses. the Personal Data Importer shall, at the request of the Personal Data Exporter, provide a copy of this written agreement and any subsequent amendments thereto to the Personal Data Exporter.

10. Compliance with These Clauses

- A. The Personal Data Importer shall respond to all inquiries and requests of the Personal Data Exporter or the Controller within the specified period and provide all information requested by the Personal Data Exporter and Controller, in addition to providing the Personal Data Exporter or the Controller with all information it may request regarding the processing of the transferred Personal Data, including any information necessary to enable

the Controller to prove its compliance with the requirements contained in these Clauses or the provisions stipulated in the Law and its Implementing Regulations before the Competent Authority.

- B. Each party is responsible for proving that all obligations under these Clauses have been fulfilled before the Competent Authority upon request, and in all cases, if the Personal Data Exporter and Data Importer violate the instructions issued by the Controller or the agreement concluded with it regarding the processing of the transferred Personal Data, the Personal Data Exporter and Data Importer shall be considered as the Controller and shall be responsible for the violation of the Standard Contractual Clauses and the provisions of the Law and the Implementing Regulations before the Competent Authority.
- C. The Personal Data Importer shall allow, without undue delay, the Personal Data Exporter or the Controller or their appointed representatives to audit the Data Importer's processing of Personal Data at the request of the Personal Data Exporter or the Controller.
- D. The Controller must provide the information revealed by the audit when requested by the Competent Authority.
- E. The right of audit does not grant the Personal Data Exporter or the Controller or their representative's access to any confidential information of The Personal Data Importer as long as this information is not closely related to the processing of the transferred Personal Data.

11. Rights of Personal Data Subjects

- A. The Personal Data Importer shall notify the Personal Data Exporter within (24) hours of receipt of any request received from the Personal Data Subject, provided that the Personal Data Exporter shall notify the Controller within

- (24) hours of receipt of the Data Importer's notification, provided that the Personal Data Importer and the Personal Data Exporter shall not respond to the request unless the Controller authorizes it to do so.
- B. The Personal Data Importer shall take all necessary measures, in cooperation with The Personal Data Exporter and the Controller, to respond to the requests of Personal Data Subjects to exercise their rights under the provisions of the Law and Regulations.
- C. The Personal Data Importer is obliged to follow all instructions issued by the Personal Data Exporter and the Controller in all matters relating to the processing of the transferred Personal Data.
- D. All statements made to the Personal Data Subject must be presented in a clear, legible, and accessible format.

Fourth Template: Processor to Controller

1. Processing Instructions

- A. The Personal Data Exporter is obliged to process the transferred Personal Data only on the basis of written instructions from The Personal Data Importer as the Controller.
- B. The Personal Data Exporter shall immediately notify The Personal Data Importer if it is unable to comply with these instructions, or if it realizes that these instructions are contrary to the provisions of the Law and its Implementing Regulations or any other law in the Kingdom of Saudi Arabia.
- C. The Personal Data Importer shall not take an action or refrain from taking an action that would prevent the Personal Data Exporter from fulfilling its obligations under the Law and its Implementing Regulations or any other regulations in force in the Kingdom, including those regulations related to cooperation with the Competent Authority or any other regulatory body.

D. After completion of the purpose of processing Personal Data specified in Appendix (2), the Personal Data Exporter shall destroy or return the transferred Personal Data as determined by the Data Importer.

2. Data Processing Security

A. The Parties shall take the necessary organizational, administrative, and technical measures to safeguard the privacy of Data Subjects and the security of Personal Data at all stages of processing, including the security of data during their transfer, and to protect against any Personal Data breach. In assessing the level of appropriate security measures, 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, purpose or purposes of the data processing and the risks involved in the processing of Personal Data, and consider the application of encryption or de-identification, including during data transfer, to ensure that the purpose of processing Personal Data is fulfilled accordingly.

B. The Personal Data Exporter shall support the Personal Data Importer in ensuring the security of the Personal Data required under paragraph (a) above, and in the event of any Personal Data breach with respect to the transferred Personal Data processed by the Personal Data Exporter under the Standard Contractual Clauses, the Personal Data Exporter shall notify the Personal Data Importer without delay within (24) hours of becoming aware thereof and the Personal Data Importer shall assist in containing such breach.

C. The Personal Data Exporter ensures that the individuals authorized to process the transferred Personal Data are bound by the confidentiality and

protection of the information or are bound by an appropriate legal obligation on the confidentiality and protection of the information.

3. Commitment to these Clauses

- A. The Personal Data Exporter is obliged to respond to all requests of the Personal Data Importer upon request, in order to enable the Personal Data Importer to demonstrate compliance with the provisions of the Standard Contractual Clauses and the Law and its Implementing Regulations.
- B. Each party shall be responsible for demonstrating to the Competent Authority, upon request, that all obligations under these Clauses have been fulfilled.

4. Rights of Personal Data Subjects

- A. All parties shall take all necessary actions and measures and cooperate to enable Personal Data Subjects to exercise their rights stipulated in the Law and Regulations.
- 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: | Name: |
| Address: | Address: |
| Contact Information: | Contact Information: |
| Signature: | Signature: |
| Date: | Date: |
| Role [Controller/Processor] | Role [Controller/Processor] |

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

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:

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-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.



SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority