Planisware
Get innovation to market

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms part of the Planisware GTC's executed between Planisware and Customer (hereinafter the "**Agreement**"). The purpose of the DPA is to reflect the agreement about the processing of personal data, in accordance with the requirements of applicable data protection laws and regulations. Planisware and Customer shall be hereinafter referred to separately by "Party" or jointly by "Parties".

1. DEFINITIONS

Unless otherwise defined in this DPA, capitalized terms shall have the meaning set forth in the Planiware GTC's.

"**Data Controller**"	means the entity that determines the purposes and means of the Processing of Personal Data. For purposes of this DPA, Customer is the Data Controller.
"**Data Processor**"	means the entity which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Planisware is the Data Processor.
"**Data Protection Laws & Regulations**"	means all mandatory laws and regulations applicable to the Processing of Personal Data under the Planisware GTC's, including the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the laws and regulations of the European Union, the European Economic Area and their member states.
"**Data Subject**"	means an individual who is subject to Data Protection Laws and Regulations and to whom Personal Data relates.
"**Personal Data**"	means data about a specific natural person transmitted to or collected by Planisware as part of Planisware's services to Customer from which that person is identified or identifiable, as defined in Data Protection Laws and Regulations.
"**Processing**"	means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, organization, storage, retrieval, consultation, use, disclosure by transmission, blocking, or deletion.
"**Security Documentation**"	means the information provided to Customer by Planisware regarding its data security technical and organizational measures as set out in Appendix 2 hereto and as may be updated by Planisware from time to time as set forth in this DPA.
"**Security Incident**"	means an unauthorized disclosure of or access to Personal Data or an accidental or unlawful destruction, loss or alteration of Personal Data.
"**Standard Contractual Clauses**" or "**Clauses**"	means standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council implemented by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
"**Sub-processor**"	means any third party, including Planisware Affiliates, engaged by Planisware for the Processing of Personal Data.

2. PROCESSING OF PERSONAL DATA

2.1. **Customer's Processing of Personal Data**. Customer shall, in its use of the Services, comply with Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions to Planisware for the Processing of Personal Data must comply with Data Protection Laws and

Regulations. In the event where Customer grants access to the Service to End-Users or Extended Users located in jurisdictions with laws requiring data localization ("**Data Localization Countries**"), or uploads to the Service any Personal Data of any individual located in Data Localization Countries: (i) Customer acknowledges that all Personal Data from Data Localization Countries will be hosted and stored in data centers located in the EEA, and may be processed in the countries listed in Appendix 1; and (ii) Customer shall vis a vis Planisware be responsible for any data localization requirement under any applicable data privacy and localization laws of Data Localization Countries.

2.2. **Planisware's Processing of Personal Data**. Planisware will process and use Personal Data on behalf of and in accordance with instructions (including via email) of Customer, and to the extent required by law. Customer hereby acknowledges that by virtue of using the Services it gives Planisware instructions to process and use Personal Data in order to provide the Services in accordance with the Agreement and as further described in Appendix 1 to this DPA. In the event of any material update in Planisware's processing of Personal Data, Planisware will immediately notify the Customer of such updates. Planisware shall immediately inform the Controller if, in its opinion, an instruction infringes Data Protection Laws and Regulations.

2.3. **Data Protection Impact Assessment**. Upon Customer's request, Planisware shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Planisware. Planisware shall provide reasonable assistance to Customer in the event of a prior consultation with or required response to enquiries from any competent data protection authority.

3. RIGHTS OF DATA SUBJECTS

3.1. **Deletion of Personal Data**. Upon termination of the Agreement for any reason whatsoever, Planisware will delete all Personal Data Processed according to this DPA or anonymize End-User data so as to remove any Personal Data as soon as reasonably practicable and request corresponding deletion/anonymization from its Sub-processors, provided that Planisware may retain data necessary to evidence compliance with applicable legal and regulatory requirements and recordkeeping.

3.2. **Data Subject Rights**. Customer is solely responsible for informing Data Subjects about the Processing of their Personal Data in accordance with Data Protection Laws and Regulations and for managing their requests to exercise their rights under Data Protection Laws and Regulations. Planisware shall, to the extent legally permitted, notify Customer in a timely manner if it receives a request from a Data Subject for access to, correction, amendment or deletion of such Data Subject's Personal Data. Planisware shall not respond to any such Data Subject request without being instructed by Customer in writing (including email) except to confirm to the Data Subject that the request relates to Customer. Customer shall be responsible for any reasonable costs arising from Planisware's provision of such assistance.

3.3. **Complaints or Notices related to Personal Data**. In the event Planisware receives any official complaint, notice, or communication that relates to Planisware's Processing of Personal Data or either party's compliance with Data Protection Laws and Regulations in connection with Personal Data, to the extent legally permitted, Planisware shall promptly notify Customer and Planisware shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from Planisware's provision of such assistance.

4. PLANISWARE PERSONNEL

4.1. **Confidentiality**. Planisware shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

Planisware shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. **Limitation of Access**. Planisware shall ensure that access to Personal Data is limited to those personnel who are authorized to do so and require such access to perform the services.

4.3. **Data Protection Officer**. Planisware has appointed a data protection officer if and whereby such appointment is required by Data Protection Laws and Regulations. Any such appointed person may be reached at dpo@planisware.com. Customer will communicate to Planisware the contact details of its DPO as soon as possible upon signature.

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors**. Customer hereby acknowledges and expressly agrees that (i) Planisware is entitled to retain its Affiliates as Sub-processors, and (ii) Planisware or any such Affiliate may respectively engage any third party to Process Personal Data on Planisware's behalf in connection with the provision of Services. Planisware will only disclose Personal Data to Sub-processors that are parties to written agreements with Planisware including obligations no less protective that the obligations of this DPA. Planisware shall ensure that access to Personal Data is limited to those Sub-processors who require such access to perform their services to Planisware for the provision of the Services to Customer. Planisware will, following the Customer's written request, provide to the Customer the names of its Sub-processors processing the Personal Data and the countries outside of the European Economic Area in which such data is or may be processed, provided that such request will not be made more than once in each calendar year. The list of Sub-processors at the date of the DPA is set out in Appendix 1.

5.2. **Objection Right for new Sub-processors**. Planisware shall notify Customer in writing (including by email) prior to appointing any new Sub-processor. If Customer is legally prohibited from consenting to Planisware's use of a new Sub-processor, then Customer will notify Planisware of such prohibition in writing within ten (10) business days after receipt of Planisware's notice. Planisware will use reasonable efforts to (i) make available to Customer a change in the affected Services (ii) recommend a commercially reasonable change to Customer's configuration or use of the affected Services to avoid processing of Personal Data by said new Sub-processor, or (iii) work with the Sub-processor to ensure that any sub-processing is performed in a manner reasonably satisfactory to Customer. If the parties are not able to find a suitable solution within a reasonable period of time, which shall not exceed sixty (60) days, then Customer may terminate any applicable agreement in respect only to those Services that cannot be provided by Planisware without the use of the objected-to new Sub-processor, by providing written notice to Planisware.

5.3. **Liability**. Planisware shall be liable for the acts and omissions of its Sub-processors to the same extent Planisware would be liable if performing the services of each Sub-processor directly under the terms of this DPA, subject to any limitations set forth in the Planisware GTC's.

6. SECURITY; AUDIT RIGHTS

6.1. **Controls for the Protection of Personal Data**. Planisware will maintain appropriate technical and organizational measures, as described in the Security Documentation, against Security Incidents.

6.2. **Audit Rights**. Planisware shall respond within a reasonable period of time to any specific written questions submitted to it by Customer regarding Planisware's data security technical and organizational measures. Planisware will allow Customer to perform an on-site audit of Planisware for verification of compliance with the technical and organizational measures set forth in the Security Documentation in the following circumstances: (i) Following the notification of Customer by Planisware of a Security Incident, (ii) Customer reasonably believes that Planisware is not in compliance with its security commitments under this DPA (and in such case Customer's audit rights may not be exercised for more than once per calendar year), or (iii) such audit is required under Data Protection Laws and Regulations or required by instruction of a competent data protection authority. Any such audit must be conducted in accordance with the procedures set forth in Section 6.3.

6.3. **Audit Process**. Customer must provide at least three (3) weeks' prior written notice to Planisware of a request to audit. The scope of any audit shall be limited to Planisware's policies, procedures and controls relevant to the protection of Personal Data as set forth in the Security Documentation. All audits will be conducted via exchange of documents. Upon receipt of a written request to audit, and subject to Customer's agreement, Planisware may satisfy such audit request by providing Customer with a confidential copy of an independent auditor's report produced by Planisware that enables Customer to verify Planisware's compliance with the technical and organizational measures set forth in the Security Documentation. An audit will be conducted at Customer's sole cost and by a mutually agreed upon third party contractor who is engaged and paid by Customer, and is under a non-disclosure agreement containing confidentiality provisions obligating it to maintain the confidentiality of all audit findings as well as Planisware's Confidential Information. Before the commencement of any such audit, Planisware and Customer shall mutually agree upon the timing, duration of the audit as well as audit methodology, and executive summary information. For the avoidance of doubt, no Personal Data other than those processed on behalf of Client will be shared or disclosed by Planisware in the course of any audit. Customer shall, at no charge, provide to Planisware a full copy of all findings of the audit. In the event where, after review of documentation provided by Planisware in response to an audit request, Customer reasonably believes that Planisware is not in compliance with its Security Documentation, then Customer can request an on-site audit, with at least three (3) week's prior written notice. Planisware will provide Planisware's then-current professional services rates and estimate of time spent by Planisware staff for responding to and cooperating with auditors. Customer shall be responsible for such costs. Planisware will cooperate with the audit, including providing auditors access to Planisware security information or materials.

6.4. **Notice of Failure to Comply**. After conducting an audit under this Section 6 or after receiving an audit report from Planisware, Customer must notify Planisware of the specific manner, if any, in which Planisware does not comply with any of the security, confidentiality, or data protection obligations in this DPA or Data Protection Laws and Regulations, if applicable. Any such information will be deemed Confidential Information of Planisware. Upon such notice, Planisware will use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1. Planisware maintains Security Incident management policies and procedures, including detailed Security Incident escalation procedures as further described in the Security Documentation. If Planisware has determined that a Security Incident has occurred, Planisware will notify Customer in a timely manner and provide Customer with relevant information about the Security Incident, including, to the extent then known, the type of Customer Data involved, the volume of Customer Data disclosed, the circumstances of the incident, mitigation steps taken, and remedial and preventative action taken. Customer shall be responsible for notifying such Security Incidents to the competent data protection authority and to Data Subjects where required by Data Protection Laws and Regulations.

8. ADDITIONAL TERMS FOR TRANSFER OF PERSONAL DATA FROM THE EEA

8.1. **Standard Contractual Clauses**. All Processing of Personal Data in countries which do not ensure an adequate level of data protection as determined by the European Commission's decision of 4 June 2021 is on the basis of and subject to the Standard Contractual Clauses. For the purpose of the Standard Contractual Clauses, this DPA and the Planisware GTC's are the complete and final instructions of Customer ("data exporter") to Planisware ("data importer") for the Processing of Personal Data. In the event of inconsistencies between the provisions of the Standard Contractual Clauses and this DPA or other agreements between the Parties, the Standard Contractual Clauses shall take precedence. The terms of this DPA shall not vary Clauses in any way. In the event that the Standard Contractual Clauses are amended, replaced or repealed by

the European Commission or otherwise under Data Protection Laws and Regulations, the parties shall work together in good faith to enter into any updated version of the Standard Contractual Clauses or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Laws and Regulations.

8.2. **Schrems II Additional Measures.** In the event of a request for disclosure of Personal Data or the direct access to Personal data by a law enforcement authority or state security body of a non-EEA country ("**Government Disclosure**") that is massive, disproportionate, or indiscriminate, Planisware will notify Customer in a timely manner (to the extent permitted by applicable law). Where Planisware notifies Customer, the Parties shall discuss in good faith the additional measures and whether to notify the appropriate supervisory authority and/or suspend further transfers of Personal Data. In the event Planisware incurs any material cost in exercising recourses against a Government Disclosure, including reasonable legal fees, such costs shall be borne and reimbursed by Customer on presentation of justifying documentation.

9. LEGAL EFFECT; TERMINATION

9.1. This DPA shall only become legally binding between Customer and Planisware when fully executed and will terminate when the Agreement terminates, without further action required by either party.

10. CONFLICT

10.1. In the event of any conflict or inconsistency between this DPA and the Planisware GTC's, this DPA will prevail.

Attachments:

- **Appendix 1** – Subject matter and details of the data processing
- **Appendix 2** – Security Documentation
- If applicable, Standard Contractual Clauses
- **Appendix 3** – Optionnal clauses

APPENDIX 1 – SUBJECT MATTER AND DATA PROCESSING DETAILS

This Appendix forms part of the DPA (and/or the SCCs, where applicable)

DATA CONTROLLER is the Customer for the purpose of using Planisware's SaaS solution.

INDEPENDENT CONTROLLER Please note that Planisware processes some Customer Personal Data as an Independent Controller for the following purposes: (a) account, billing, and customer relationship management and related customer correspondence; (b) compensation (e.g., calculating employee commissions and partner incentives); (c) complying with legal obligations, (for instance tax requirements) (d) abuse detection, prevention, and protection, virus scanning, (e) creating aggregated statistical data for internal reporting. Planisware conducts such processing in compliance with Data Protection Laws & Regulations and with the Planisware Privacy Policy [https://planisware.com/privacy-policy].

DATA PROCESSOR Planisware offers a project management SaaS solution, enabling project prioritization, portfolio balancing, and capacity planning and has signed the Planisware GTC's with Customer.

SUB-PROCESSORS In accordance with clause 5.1, Planisware may retain its Affiliates as Sub-processors, and any such Affiliate may respectively engage any third parties to process Personal Data in connection with the provision of Services. The Sub-processors are the following (to the exception of the Planisware signing entity):

NAME	LOCATION	ACTIVITIES RELEVANT TO THE PROCESSING
Planisware S.A	200 avenue de Paris, 92320 Chatillon, France	Providing support services to End-Users of Customer
Planisware USA Inc.	555 Montgomery Street, Suite 1300 San Francisco, California , 94111 United States	
Planisware Deutschland GmbH	52-58 Leonrodstrasse, 80636 München, Germany	
Planisware UK Ltd.	11.14 - 11.17, Level 11 Blue Tower, Media City Uk, Salford, England, M50 2ST T	
Planisware Singapore Pte Ltd.	600 North Bridge Rd, #10-01, Singapore 188778	
PLW Tunisia SUARL	56 boulevard de la Corniche Avenue de Beji Caid Essebsi, Lac II, 1053 Tunis, Tunisia	
Planisware MIS SARL	5 rue du Helder, 75009 Paris, France	
Planisware MIS (DMCC Dubaï Branch)	Unit 1902 - The Dome Tower | JLT-PH1-N1 - Jumeirah Lakes Towers	
Planisware Belgium	Avenue des Volontaires 19 1160 Auderghem	
Planisware Korea LLC	354, Gangnam-daero, Gangnam-gu, Seoul, 11F, SW55	
Planisware Japan KK	10th Floor, PMO Kojimachi, 6-2-6 Kojimachi, Chiyoda-ku, Tokyo, 102-0083 Japon	
Planisware MIS	MirMar Business City, Centre Urbain Nord, 1003 Tunis, Tunisia	Providing support services to End-Users of Customer as well as managed services, where applicable

DATA SUBJECTS

The Data Controller may submit Personal Data to Planisware, the extent of which is determined and controlled by the Data Controller in its sole discretion, and which include the following categories of data subjects:

1. Employees of the Data Controller
2. Independent contractors of the Data Controller
3. Other End-Users as the Data Controller authorizes under the Agreement
4. Any individual whose Personal Data is Processed by the Controller through projects managed with Planisware project management SaaS solution.

CATEGORIES OF DATA

The Personal Data transferred concern the following categories of data:

1. The categories of Personal Data Processed to access the Services:
    - First and last name
    - End-User ID
    - End-User email
    - IP address
    - Job titles/roles
2. Activity of End-User in connection with Customer's account,
3. Communication between End-Users and Planisware staff in connection with support services,
4. Where applicable, communication between End-Users and Planisware staff in connection with Professional Services.

SPECIAL CATEGORIES OF DATA

Customer must not use the Services to process Personal Data deemed special categories of data under Data Protection Laws and Regulations without prior agreement of Planisware's signatory of this DPA.

PROCESSING OPERATIONS

The Personal Data processed will be subject to the following basic Processing activities:

1. Collecting, hosting and back-up storage of personal data for purposes of:
    - Recognizing authorized End-User of the Service
    - Enabling administration of Customer account by data exporter
    - Providing support services to End-Users
    - Where applicable, providing professional services
2. Deletion or anonymization of Personal Data upon instruction of Customer or at the end of the Agreement.

Planisware
Get innovation to market

APPENDIX 2 – SECURITY DOCUMENTATION

This Appendix forms part of the DPA (and/or the SCCs, where applicable)

DESCRIPTION OF THE TECHNICAL AND ORGANISATIONAL SECURITY MEASURES IMPLEMENTED BY PLANISWARE

As per Article 32 of the GDPR, Planisware has implemented and maintains a comprehensive written information privacy and security program (including provisions regarding retention of records and incident response plan) that includes appropriate administrative, organizational, technical and physical safeguards and other security measures appropriate to the size and complexity of the data processing, the harm that might result from a Security Incident and the nature and scope of the personal data processing activities. Planisware may update these technical and organizational security measures from time to time so long as they do not materially decrease the overall security of the personal data processing.

1. PSEUDONYMISATION OF PERSONAL DATA/ENCRYPTION OF PERSONAL DATA

Measures are used to ensure that personal data cannot be read, copied, modified or deleted without authorisation during electronic transmission or transport, and that the target entities for any transfer of personal data by means of data transmission facilities can be established and verified.

2. ABILITY TO ENSURE THE ONGOING CONFIDENTIALITY AND INTEGRITY OF PROCESSING SYSTEMS AND SERVICES

2.1 Measures to prevent unauthorized persons from gaining physical access to personal data processing systems:

a) Definition of persons who are granted physical access to systems where personal data is Processed;
b) Electronic access control;
c) Issuance of access IDs;
d) Implementation of policy for external individuals;
e) Alarm device or security service outside service times;
f) Division of premises into different security zones;
g) Implementation of key(-card) handling policy;
h) Security doors (electronic door opener);
i) Implementation of measures for on-premise security (e.g. intruder alert/notification).

2.2 Measures to prevent unauthorized persons from using personal data processing equipment:

a) Definition of persons who may access personal data processing equipment;
b) Implementation of policy for external individuals;
c) Password protection of personal computers.

2.3 Measures ensuring that persons entitled to use a data processing system gain access only to such personal data as they are entitled to accessing in accordance with their access rights:

a) Implementation of access rights for respective personal data and functions;
b) Requirement of identification vis-à-vis the data processing system (e.g. via ID and authentication);
c) Implementation of policy on access- and user-roles;
d) Evaluation of protocols in case of damaging incidents.

2.4 Measures such as logging of data entry, to ensure that it is possible to check and ascertain whether personal data have been entered into, altered or removed from personal data processing systems and if so, by whom.

2.5 Measures to ensure that personal data processed on behalf of others are Processed in compliance with Customer's (data controller and data exporter) instructions, including training of Planisware personnel and documentation of Customer support requests.

2.6 Measures to ensure that personal data collected for different purposes can be processed separately such as the use of logical separation of personal data of each of data processor's clients.

3. ABILITY TO ENSURE THE AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

Measures to ensure that personal data is protected against accidental destruction or loss:

a) Realization of a regular backup schedule;
b) Control of condition of data carriers for personal data backup purposes;
c) Safe storage of personal data backups;
d) Implementation and regular control of emergency power systems and overvoltage protection systems.

4. ABILITY TO RESTORE THE AVAILABILITY TO ACCESS PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT

Measures to ensure that personal data can be restored in a timely manner in the event of accidental destruction or loss:

a) Implementation of an emergency plan;
b) Protocol on the initiation of crisis- and/or emergency management.

5. PROCEDURES FOR REGULAR TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANIZATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING

a) Regular review of IT security related certifications (e.g. ISO 27001);
b) Monitoring by Planisware's Data Protection Officer, if designated, and IT review concerning the compliance with the determined processes and requirements for the configuration and operation of the systems.

APPENDIX 3 – [Optional] Region-specifics

This Appendix forms part of the DPA.

Abu Dhabi. Where Personal Data protected by Abu Dhabi Data Protection Laws & Regulations is transferred, either directly or via onward transfer,the following addendum to the EU SCC's will apply: https://assets.adgm.com/download/assets/ADGM+-+Data+Transfer+Addendum+to+the+EU+SCC-pdf.pdf/9e08f13a595b11efb0b3aa2a20d5f45b

Argentina. Where Personal Data protected by Argentina Data Protection Laws & Regulations is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the following SCC's will apply: http://www.jus.gob.ar/media/3202473/disp_e2016_60_anexoii.pdf

California. Where Personal Data protected by the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA") is processed by Planisware, Planisware will process Personal Data only for business purposes and operational purposes applicable to the Customer's instructions that are permissible under the CCPA for a service provider and not for Planisware's own purposes (as all such terms are defined in the CCPA). Planisware shall not use or process any Personal Data outside of the scope of the Services or its relationship with Customer. Planisware will not use any Personal Data for direct marketing purposes nor sell or share any Personal Data, as selling or sharing is defined in the CCPA. Planisware will not combine Personal Data received from Customer with the personal data it receives from other sources. In the event of any material update in Planisware's processing of Personal Data, Planisware will immediately notify the Customer of such updates. Planisware certifies that it understands and will comply with the foregoing restrictions.

Dubai. Where Personal Data protected by Dubai Data Protection Laws & Regulations is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the following SCC's available for download will apply: https://www.difc.com/business/registrars-and-commissioners/commissioner-of-data-protection/data-export-and-sharing

Turkey. Where Personal Data protected by Turkey Data Protection Laws & Regulations is transferred, either directly or via onward transfer, the following SCC's will apply: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/d4577ac6-d2cd-4ff4-839f-4218812c3cdc.pdf

United Kingdom. Where Personal Data protected by UK Data Protection Laws & Regulations is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the following UK Addendum to the EU SCC's will apply: https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf

Switzerland. Where Personal Data protected by Swiss Data Protection Laws & Regulations is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the following Swiss Addendum to the EU SCC's will apply:

" Where a transfer of personal data from a Data Exporter to a Data Importer is subject to the EU GDPR and the FADP (Federal Act on Data Protection of 25 September 2020 - last amended on 7 July 2025), the following additional provisions shall also apply in order for the Standard Contractual Clauses to be suitable for ensuring an adequate level of protection for such transfer in accordance with Article 6 paragraph 2 letter of the FADP:

The term "EU Member State" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses.

The Federal Data Protection and Information Commissioner is the competent supervisory authority with regard to the transfer of personal data out of Switzerland."

Saudi Arabia. Where Personal Data protected by Saudi Arabia Data Protection Laws & Regulations is transferred, either directly or via onward transfer, the following Standard Contractual Clauses will apply: https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf