

## DATA PROTECTION ADDENDUM

### 1 DEFINITIONS

1.1 The following terms apply to this Data Protection Addendum ("DPA") in addition to those defined in the EU General Data Protection Regulation ("GDPR"):

<b>"Agreement"</b>	means any agreement and any attachment for the delivery of Services that is entered into between the Customer (being the Controller) and the Supplier (being the Processor) whereby this DPA reflects the parties' agreement with regard to the processing of personal data.
<b>"Applicable Data Protection Law"</b>	means any data protection law that applies to Customer's processing of personal data such as but not limited to the EU General Data Protection Regulation ("GDPR"), the UK Data Protection Act ("UK GDPR"), the California Consumer Privacy Act ("CCPA"), the Swiss Federal Act on Data Protection ("FADP"), the Brazilian General Data Protection Law ("LGPD") and the South African Protection of Personal Information Act ("POPIA").
<b>"Services"</b>	means services carried out by Supplier on behalf of Customer as set out in the Agreement and the Appendix to this DPA.
<b>"Standard Contractual Clauses" ("SCCs")</b>	means the EU Standard Contractual Clauses adopted by the European Commission for the transfer of personal data to third countries as currently effective. To the extent transfers of personal data originate from the UK, the parties agree that the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses shall also apply. To the extent transfers of personal data originate from Switzerland, the parties agree that, for purposes of the EU Standard Contractual Clauses: (i) the term 'member state' shall be interpreted to include Switzerland and, for the avoidance of doubt, the term 'data subject' includes residents of Switzerland; (ii) references to the GDPR are to be interpreted as including a reference to the FADP; and (iii) for data transfers subject solely to the FADP, the Swiss Federal Data Protection Authority is the competent supervisory authority, and disputes arising from such transfers may be brought in the courts of Switzerland.
<b>"Subprocessor"</b>	means a sub-contractor that Supplier engages to process personal data on behalf of Customer when carrying out the subcontracted Services.
<b>"Restricted Transfer"</b>	means a transfer of personal data originating in the EEA, UK or Switzerland that is subject to GDPR, UK GDPR and/or the FADP to a third country, where any required adequacy means can be met e.g. by entering into the SCCs.

### 2 DETAILS OF PROCESSING

2.1 The Appendix to this DPA details the processing operations that Supplier provides to Customer.

### 3 OBLIGATIONS OF CUSTOMER

3.1 Customer shall comply with Applicable Data Protection Law and demonstrate such compliance as required under the Applicable Data Protection Law.

### 4 INSTRUCTIONS

4.1 Customer instructs Supplier to process personal data on its behalf for the purposes of performing the Services. Customer shall ensure that any instruction given to Supplier complies with Applicable Data Protection Law. If Customer acts as a processor to another controller, Customer warrants that its instructions and actions with respect to the processing of the personal data provided to the Supplier have been authorized by the relevant controller.

4.2 Supplier shall process personal data only in accordance with the instructions given by the Customer unless otherwise required by Applicable Data Protection Law.

4.3 Any further instructions that go beyond the instructions contained in this DPA or the Agreement must be within the subject matter of this DPA and the Agreement. If the implementation of such further instructions results in costs for Supplier, Supplier shall inform Customer about such costs before implementing the instructions. Only after Customer's confirmation to bear such costs, Supplier is required to implement such further instructions. Customer shall give further instructions generally in written form (electronic form is sufficient), unless the urgency or other specific circumstances require another (e.g., oral) form. Instructions in another form shall be confirmed by Customer in written form without delay.

4.4 Supplier shall immediately inform Customer if, in its opinion, an instruction infringes the Applicable Data Protection Law and request Customer to withdraw, amend or confirm the relevant instruction. Supplier shall be entitled to suspend implementation of the relevant instruction pending Customer's decision to withdraw, amend or confirm such instruction.

### 5 OBLIGATIONS OF SUPPLIER

5.1 Supplier shall ensure that all persons authorized by Supplier to process personal data on behalf of Customer, particularly Supplier's or any Subprocessor's staff, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.2 The Supplier will not combine personal data received from, or on behalf of, Customer with personal data that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

5.3 Supplier shall implement and maintain reasonable security practices and procedures appropriate to the nature of the personal data to protect it from unauthorized or illegal access, destruction, use, modification, or disclosure. Before processing personal data to provide the Services, Supplier shall implement the technical and organizational measures documented at ARIS Trust Center: <https://trust.aris.com/item/data-processing-agreement>. Supplier may amend the technical and organizational measures from time to time provided that the amended technical and organizational measures are not less protective than those in place as of date that the parties concluded this DPA.

5.4 Supplier shall make available to Customer all information necessary to demonstrate compliance with the obligations in the Applicable Data Protection Law. The parties agree that this information obligation is met by providing Customer with an audit report or equivalent documentation upon request. To the extent additional audit activities are required by Applicable Data Protection Law or by order of a competent authority, Customer may request additional audits to be carried out by the Customer itself, or an auditor appointed by it.

5.5 Any on-site audit must:

- (a) be limited to processing facilities and Supplier's staff involved in the processing activities covered by this DPA;
- (b) occur no more than once annually or as required by Applicable Data Protection Law or by a competent authority or immediately after a material personal data breach affecting personal data processed by Supplier under this DPA; and
- (c) may occur only during regular business hours, after reasonable prior notice, in accordance with Supplier's security policies and without substantially disrupting Supplier's business operations.

Each Party shall bear its own costs arising out of or in connection with any on-site audit. Customer shall create and provide to Supplier with an audit report summarizing the findings and observations of the on-site audit. Any such audit report is confidential information and may not be disclosed to third parties unless required by Applicable Data Protection Law, order of a competent authority or with Supplier's consent.

- 5.6 Supplier shall notify Customer without undue delay:
- (a) about any legally binding request for disclosure of Customer's personal data by a law enforcement authority, unless prohibited by applicable law;
  - (b) if applicable law requires Supplier to process personal data beyond Customer's instructions, or if Supplier determines that it can no longer meet its obligations under Applicable Data Protection Law, unless applicable law prohibits such information. Upon notice, Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of personal data; and
  - (c) in the event a personal data breach has occurred at Supplier or at a Subprocessor that may affect the Customer's personal data processed under this DPA. In this case, Supplier shall assist Customer with its obligation under Applicable Data Protection Law to inform the data subjects and/or the competent authorities, as applicable, by providing information in accordance with Applicable Data Protection Law as available to Supplier. Supplier shall implement suitable remediation measure to prevent future breaches.
- 5.7 Supplier shall take commercially reasonable measures to provide necessary information and assist Customer with its accountability obligations, such as but not limited to a data protection impact assessment or prior consultation in relation to the Services, as may be required by Applicable Data Protection Law. Supplier must provide such assistance only if required by Applicable Data Protection Law or if Customer cannot meet its obligation through other means.
- 5.8 At the choice of Customer, Supplier shall delete or return to Customer all personal data (including any data storage media) processed on Customer's behalf under this DPA after the end of the provision of Services and delete any existing copies unless applicable law requires Supplier to retain such personal data.

## **6 DATA SUBJECT RIGHTS**

- 6.1 Customer is primarily responsible for handling and responding to requests made by data subjects. If a data subject contacts Supplier directly, Supplier shall communicate the data subject's request to Customer. Supplier shall not respond to any data subject independently.
- 6.2 Supplier shall assist Customer in responding to data subjects' requests to exercise their rights set out in Applicable Data Protection Law.

## **7 SUBPROCESSING**

- Supplier will only engage a Subprocessor to assist the Supplier in providing the Services to Customer under the Agreement in accordance with the underlying DPA. Customer authorizes the use of Subprocessors for the provision of the Services under this DPA. The same applies to the use of further sub-processors engaged by Subprocessors, in which case the below applies accordingly. Supplier shall choose such Subprocessor diligently. Supplier remains responsible for any acts or omissions of its Subprocessors in the same manner as for its own acts and omissions hereunder. Customer approves the Subprocessors documented at ARIS Trust Center: <https://trust.aris.com/>.
- 7.1 Supplier shall pass on in writing (electronic form is sufficient) to Subprocessors the Supplier's obligations under this DPA to the extent applicable to the subcontracted Services.
- 7.2 Supplier may replace or appoint suitable and reliable Subprocessors at its discretion. Supplier shall after Customer's online registration to Trust Center Updates at <https://trust.aris.com/> notify Customer in advance of any changes to its Subprocessor(s). If Customer does not object within 30 days of receiving Supplier's notice the Subprocessor(s) are deemed accepted. If Customer has a legitimate reason to object to a Subprocessor, Customer shall notify Supplier thereof in written form within the aforementioned period. If the Customer objects to a Subprocessor, the Supplier may remedy the objection within 30 days of receiving the Customer's notice. If the objection has not been cured, either party may terminate the affected Service with reasonable written notice.
- 7.3 In exceptional cases being outside of Supplier's reasonable control, Supplier may replace a Subprocessor without advance notice for urgent reason to ensure seamless Service provision, or security of personal data. Supplier will notify Customer without undue delay, and Customer shall retain the right to object to such replacement under the terms of this DPA.

## **8 RESTRICTED TRANSFER**

- 8.1 When the transfer of personal data is a Restricted Transfer, it shall be performed in compliance with Applicable Data Protection Law. The Customer agrees that where engaging a Subprocessor in accordance with this DPA causes a Restricted Transfer, the Supplier and the Subprocessor may ensure compliance with Applicable Data Protection Law by using the SCCs and to the extent legally required supplementary contractual, organizational and technical measures to provide a sufficient level of data protection.

## **9 US State Privacy Laws**

- 9.1 Notwithstanding the foregoing, the provisions of this clause solely apply to the processing of personal data relating to residents of the United States of America and, as a result of such residency, are subject to applicable US state privacy laws.
- 9.2 To the extent that the processing of personal data is subject to US state privacy laws, including but not limited to the CCPA (together "Applicable US Privacy Law"), the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" apply and shall have the meanings as set forth in the CCPA. All references to "Customer," "Supplier," "personal data" and "data subject" in the DPA shall be deemed to be referenced to "Business," "Service Provider," "Personal Information" and "Consumer," respectively, as defined in the CCPA. All terms shall be interpreted to include and apply to all residents of any US Federal State.
- 9.3 The parties acknowledge and agree that the Supplier is a Service Provider receiving Personal Information from Customer solely to provide the Services pursuant to the Agreement, which constitutes a Business Purpose. The Customer shall disclose Personal Information to the Supplier only for the limited and specified purposes described in the Agreement.
- 9.4 The Supplier shall
- (a) not Sell or Share Personal Information provided by Customer under the Agreement.
  - (b) not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by Applicable US Privacy Law.
  - (c) not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement outside of the direct business relationship between the Supplier and Customer, except where and to the extent permitted by Applicable US Privacy Law.
  - (d) comply with all obligations applicable to Service Providers under Applicable US Privacy Law, including by providing Personal Information provided by Customer under the Agreement the level of privacy protection required by Applicable US Privacy Law.

## **10 TERM**

- 10.1 This DPA shall remain in effect for each term of an Agreement entered into between the parties.

## **11 GENERAL**

- 11.1 Any liability arising out of or in connection with a violation of the obligations of this DPA or under Applicable Data Protection Law, shall follow, and be governed by, the liability provisions set forth in, or otherwise applicable to, the Agreement, unless otherwise provided within this DPA.
- 11.2 In the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, the provisions of this DPA will prevail regarding the parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the parties' data protection obligations, this DPA will prevail. If any provision of this DPA is held to be invalid, illegal or unenforceable, the remaining provisions shall not be affected or impaired.

**APPENDIX: DETAILS OF PROCESSING**

<b>Processing Operations</b>	<b>Cloud Services:</b> The Customer is a user of certain Cloud Services provided by the Supplier. The Supplier processes Customer's business data, which may contain personal data, with a Software as a Service /Platform as a Service /Software operated as a Service in a public cloud infrastructure as defined in the Agreement.
	<b>Support Services:</b> The Supplier carries out technical support for its Services. This includes solution of support incidents reported by the Customer, which may require processing of Customer's personal data to analyze or reproduce incidents.
	<b>Professional Services:</b> The Supplier supports the Customer in implementing the Supplier's software solutions and optimizing their business processes. In that matter the Customer may provide grant access to Customer's personal data. The Supplier will access or process the Customer's personal data only as defined in the Agreement.
<b>Data subjects</b>	The relevant data subjects include the individuals about whom personal data is processed in line with Service provision by the Supplier. The extent of which is determined and controlled by the Customer and may include the following categories: <ul style="list-style-type: none"> <li>• employees of Customer</li> <li>• end-customers of Customer</li> <li>• potential end-customers of Customer</li> <li>• any person with whom Customer maintains a business relationship</li> </ul>
<b>Categories of personal data</b>	The categories of personal data processed by the Supplier are determined and controller by the Customer and may include the following categories: <ul style="list-style-type: none"> <li>• Name</li> <li>• Corporate Personnel ID</li> <li>• Business e-mail address</li> <li>• Telephone number</li> <li>• Data of the Controller used within the systems which are in the scope as defined in the relevant Statement of Work</li> <li>• Data of the Controller used within the products offered by Processor</li> </ul>
<b>Special categories of data</b>	The categories of personal data processed by the Supplier are determined and controller by the Customer. The processing of special categories of personal data is not anticipated.
<b>Subject matter of the processing</b>	<b>Cloud Services:</b> The subject matter of the data processing under this DPA are the Customer's personal data processed in the Cloud Services as defined in the Agreement including the operation of a Cloud Service platform. To access the operated platform, users need to be authenticated and authorized. User details will be used to create unique user IDs that are used for authentication and authorization. Email addresses might be used to send notifications to the users as result of using services of the Cloud Service platform and corresponding support systems (e.g., Ticket system).
	<b>Support Services:</b> As described in the applicable Maintenance and Support Service description.
	<b>Professional Services:</b> The subject matter of the processing as described in the relevant Statement of Work.
<b>Nature and purpose of the processing</b>	<b>Cloud Services:</b> The purpose of the data processing under this DPA is the provisioning of the Cloud Services initiated by the Customer. The Cloud Services processing systems and respective processing properties are defined in the Agreement.
	<b>Support Services:</b> Supplier processes personal data of the data subjects on behalf of the Customer in order to solve support incidents in Supplier's software products.
	<b>Professional Services:</b> Supplier processes personal data of the data subjects on behalf of the Customer in order to provide Professional Services described in detail in the relevant Statement of Work.