Sairis LLC Data Processing Addendum

This Addendum was last updated on June 01, 2025.

Sairis LLC, ("Sairis")

PURPOSE

This Data Processing Addendum, including its Schedules, ("DPA") forms part of the Main Services Agreement or other written or electronic agreement between Sairis and Customer for the purchase of Services (including associated Sairis offline or mobile components) from Sairis (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") (the "Agreement") to reflect the Parties' agreement with regard to the Processing of Personal Data. It is applicable when Data Protection Laws apply to Customer's use of Services to Process Personal Data. In consideration of the mutual obligations in this DPA, the Parties agree that the terms of this DPA will form part of the Agreement, which will remain in full force and effect except as modified below.

In the course of providing the Services to Customer pursuant to the Agreement, Sairis may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Sairis entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with Sairis or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Form(s), and the Sairis entity that is party to such Order Form is party to this DPA. For the purposes of this DPA, any reference to Order Form herein shall include "Ordering Document" (as defined in the Agreement).

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

If the Customer entity signing the DPA is not a party to an Order Form nor an Agreement directly with Sairis, but is instead a customer indirectly via an authorized reseller of Sairis services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

1. **DEFINITIONS**

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Sairis, but has not signed its own Order Form with Sairis.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, as amended by the California Privacy Rights Act, and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Customer**" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and its Authorized Affiliates.

"Customer Data" means what is defined in the Agreement as "Customer Data" or "Your Data", provided that such data is electronic data and information submitted by or for Customer to the Services. This DPA does not apply to Content or Non-Sairis Applications as defined in the Agreement or, if not defined in the Agreement, as defined in the Main Services Agreement at https://www.Sairis.ai/legal.

"Data Protection Laws and Regulations" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including but not limited to the General Data Protection Regulation (GDPR), the UK Data Protection Act, the California Consumer Privacy Act (CCPA), the Colorado Privacy Act (CPA), and similar data protection laws in the United States and globally.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"**Europe**" means the European Union, the European Economic Area, Switzerland and the United Kingdom.

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"Processing" or **"Process"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"**Public Authority**" means a government agency or law enforcement authority, including judicial authorities.

"Professional Services Security, Privacy and Architecture Documentation" means the Security, Privacy and Architecture Documentation applicable to the Professional Services purchased by Customer, as updated from time to time, and accessible via Sairis' Legal webpage at https://www.Sairis.ai/legal, or otherwise made reasonably available by Sairis.

"Sairis" means the Sairis LLC entity which is a party to this DPA.

"Sairis Group" means Sairis and its Affiliates engaged in the Processing of Personal Data.

"Standard Contractual 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 the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

"Sub-processor" means any Processor engaged by Sairis or a member of the Sairis Group.

"**User**" means, in the case of an individual accepting these terms on his or her own behalf, such individual, or, in the case of an individual accepting this Agreement on behalf of a company or other legal entity, an individual who is authorized by Customer to use a Service, for whom Customer has purchased a subscription (or in the case of any Services provided by Sairis without charge, for whom a Service has been provisioned), and to whom Customer (or, when applicable, Sairis at Customer's request) has supplied a user identification and password (for Services utilizing authentication). Users may include, for example, employees, consultants, contractors and agents of Customer, and third parties with which Customer transacts business.

2. PROCESSING OF PERSONAL DATA

2.1. **Customer's Processing of Personal Data.** Customer as Controller or Processor shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of Sairis as Processor (including where the Customer is a Processor, by ensuring that the ultimate Controller does so). For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Laws and Regulations.

2.2. **Sairis' Processing of Personal Data.** Sairis shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. Sairis shall not retain, use, or disclose Personal Data for any purpose other than as specified in the Agreement, including any internal use unrelated to the provision of Services, unless expressly permitted by applicable Data Protection Laws or with Customer's prior written instruction.

2.3. **Details of the Processing.** The subject-matter of Processing of Personal Data by Sairis is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Description of Processing/Transfer) to this DPA.

2.4. **Customer Instructions**. Sairis shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the GDPR and/or (ii) if Sairis is unable to follow Customer's instructions for the Processing of Personal Data.

2.5. **Exceptional Data**. Customer acknowledges that the nature of the Services provided by Sairis include opportunities for Customer and its Users to upload content and data in various formats to Sairis Services, including through AI processing workflows, outside of the standard intention and purposes of this DPA. Customer shall indemnify, defend, and hold harmless Sairis, its Affiliates, officers, directors, employees, and agents from and against any and all claims, damages, losses, costs, liabilities, fines, penalties, and expenses (including reasonable attorneys' fees and costs) arising from or relating to: (a) Customer's or its Users' upload, transfer, or processing of special categories of data, sensitive personal information, or any data that violates applicable Data Protection Laws and Regulations; (b) any regulatory fines, penalties, or enforcement actions imposed on Sairis resulting from Customer's data uploads or processing instructions; (c) any third-party claims arising from Customer's use of special category data through the Services; (d) any compliance costs, remediation expenses, or notification requirements incurred by Sairis in connection with Customer's upload or processing of such data; and (e) any breach of Data Protection Laws and Regulations caused by Customer's data or processing instructions. This indemnification obligation shall survive termination of this Agreement and applies regardless of whether Customer was aware of the nature of the uploaded data.

2.6. **AI and Machine Learning Processing**. Customer acknowledges that the Services include AI and machine learning capabilities that may process Personal Data through large language models, natural language processing, and other AI technologies. Customer warrants that all data uploaded for AI processing complies with applicable Data Protection Laws and Regulations and that Customer has obtained all necessary consents and authorizations for such AI processing. Customer shall indemnify Sairis for any claims arising from AI processing of Customer's data, including but not limited to claims related to algorithmic bias, automated decision-making violations, or unauthorized AI training on personal data.

3. RIGHTS OF DATA SUBJECTS

3.1. **Data Subject Request.** Sairis shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "**Data Subject Request**". Sairis shall not respond to a Data Subject Request itself, except that Customer authorizes Sairis to redirect the Data Subject Request as necessary to allow Customer to respond directly.

3.2. **Required Assistance.** Taking into account the nature of the Processing, Sairis shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

3.3. **Additional Assistance.** To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Sairis shall upon Customer's written request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Sairis is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for costs arising from Sairis' provision of assistance that exceeds standard support obligations. Standard assistance included at no additional cost includes: (a) providing existing standard reports and documentation; (b) up to four (4) hours of technical consultation per calendar quarter; (c) standard data export functionality available through the Services interface; and (d) basic guidance on data subject request procedures. Additional assistance subject to Customer cost responsibility at $300 per hour includes: (a) custom report generation or data analysis; (b) technical consultation exceeding the quarterly allowance; (c) specialized data formatting, transformation, or manual data extraction; (d) assistance requiring specialized legal or compliance expertise; and (e) any assistance requiring more than eight (8) hours of Sairis personnel time per individual request.

4. SAIRIS PERSONNEL AND DATA PROTECTION OFFICER

4.1. **Confidentiality, Reliability and Limitation of Access.** Sairis 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. Sairis shall (i) ensure that such confidentiality obligations survive the termination of the personnel engagement; (ii) take commercially reasonable steps to ensure the reliability of any Sairis personnel engaged in the Processing of Personal Data; and (iii) ensure that Sairis' access to Personal Data is limited to those personnel performing Services in accordance with the Agreement, any applicable Order Form(s) and Documentation.

4.2. **Data Protection Officer.** Members of the Sairis Group have appointed a data protection officer. The appointed person may be reached at privacy@sairis.ai.

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Sairis' Affiliates may be retained as Sub-processors; and (b) Sairis and Sairis' Affiliates respectively may engage third-party Sub-processors to provide the Services. Sairis or a Sairis Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2. **Current List of Sub-processors and Notification of New Sub-processors.** The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description of their processing activities and countries of location, is listed under the Infrastructure and Sub-processor Documentation which can be found on Sairis' Legal website at https://www.Sairis.ai/legal Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data.

5.3. **Objection Right for New Sub-processors.** In accordance with CPA and other applicable laws, Sairis will provide notice and an opportunity to object to the use of new Sub-processors. Customer may, at their sole discretion, review the list of Sub-processors at any time. Sairis will notify Customer of any change in Sub-processors by updating the Sub-processor list, including the addition or replacement of Sub-processors, thereby giving the Customer the opportunity to object to such changes. Customer may object to Sairis' use of a new Sub-processor by notifying Sairis promptly in writing within thirty (30) days of the Sub-processor list being updated. If, within 30 business days of the Sub-processor list being updated the Customer has not objected to the intended change via written notification to the Sairis Data Protection Officer, the Customer is deemed to have authorized the intended change. If Customer objects to a new Sub-processor via written notification as permitted in this clause, Sairis will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Sairis is unable to make

available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Sairis without the use of the objected-to new Sub-processor by providing written notice to Sairis. Sairis will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer

5.4. **Sairis Cloud Service Providers.** Customer acknowledges that in order to provide its Services, Sairis engages third-party service providers, including primarily, but not limited to, cloud service providers such as Amazon Web Services ("AWS"). AWS operates as a Sub-processor under this DPA and is committed to maintaining high standards of data protection and compliance. AWS's Data Processing Addendum (DPA), detailing their compliance with GDPR and other data protection regulations, is incorporated into this agreement by reference and can be reviewed at https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf along with the Supplementary Addendum to AWS Data Processing Addendum which can be reviewed at https://d1.awsstatic.com/Supplementary_Addendum_to_the_AWS_GDPR_DPA.pdf. For purposes of additional information on AWS's cloud services and how it's security standards and services provide additional security measures for Sairis, such documentation can be reviewed at https://docs.aws.amazon.com/.

5.5. **Liability.** Sairis shall be liable for the acts and omissions of its Sub-processors to the same extent Sairis would be liable if performing the services of each Sub-processor directly under the terms of this DPA, and only to the extent that such act and omission by its Sub-processors is directly related to the Sairis Services utilized by Customer for the processing of personal data in accordance with this Agreement, unless otherwise set forth in the Agreement.

6. SECURITY, CERTIFICATIONS AND AUDIT

6.1. **Controls for the Protection of Customer Data.** Sairis shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in this Agreement. Sairis regularly monitors compliance with these measures. Sairis will not materially decrease the overall security of the Services during a subscription term.

6.2. **Access to Third-Party Certifications and Audits Information.** Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Sairis shall provide Customer with a report and/or confirmation of Sairis' audits of third-party Sub-processors' compliance with the data protection controls set forth in this DPA and/or a report of third-party auditors' audits of third party Sub-processors that have been provided by those third-party Sub-processors to Sairis, to the extent such reports or evidence may be shared with Customer ("Third-party Sub-processor Audit Reports"). Customer acknowledges that (i) Third-party Sub-processor Audit Reports shall be considered Confidential Information as well as confidential information of the third-party Sub-processor and (ii) certain third-party Sub-processors to Sairis may require Customer to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

6.3. **On-Site Audit**. In accordance with Data Protection and Compliance Policies, including GDPR and the Colorado Privacy Act (CPA) § 6(1)(d) Sairis allows for, cooperates with, and contributes to audits, including inspections, solicited by and conducted by Customer or an external auditor engaged by Customer. Audits may be conducted: (i) from time to time upon written notice of 60 days or more in advance of the requested Audit, but no more than once annually; (ii) during normal business hours and so as not to unreasonably interfere with Sairis' performance of the Services under the Agreement or unreasonably interfere with Sairis' business; and (iii) during the term of this DPA and applicable Order Form; and (iv) any on-site audits will be limited to Customer Data Processing and Storage Facilities operated by Sairis related to the Services processing Customer's data which are under audit and may not include Data Processing and Storage Facilities owned or operated by Sairis' Sub-processors; and (v) Customer will bear all costs related to both parties upon Customer's solicitation of an audit. The notice and cost requirement in this section will not apply to the extent the audit is initiated by a regulator (unrelated to and unrequested by Customer) or is requested due to a Personal Data Breach. If an emergency justifies a shorter notice period, Sairis will use good faith efforts to accommodate the On-Site Audit request granted it is (i) during Sairis' normal business hours; and (ii) under reasonable duration; and (iii) shall not unreasonably interfere with Sairis' day-to-day operations. Customer's cost responsibility shall be subject to the following limitations: (a) Sairis personnel costs shall not exceed $350 per hour for senior technical staff, $250 per hour for technical staff, and $150 per hour for administrative support; (b) Customer's total cost obligation for any single audit shall not exceed $50,000 unless Customer provides written authorization for additional costs; (c) if audit duration exceeds seven (7) business days due to Customer's requests, scope changes, or requirements, Customer shall pay additional costs at the rates specified above; (d) Customer shall provide a

purchase order or written cost authorization before audit commencement if estimated costs exceed $15,000; and (e) Sairis may suspend audit activities if costs approach the specified limits until Customer provides additional authorization.

6.4. **Scope of Audit.** Before any On-Site Audit commences, Customer and Sairis shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Sairis. Sairis shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Sairis customers' information. Sairis will provide to Customer, its auditors, and regulators reasonable assistance so they can perform an audit, including permitting them access to the following: the place, premises, and facilities from which the Services will be performed; the systems (including software, networks, firewalls, and servers) used to perform the Services; and data, records, manuals, and other information relating to the Services. Sairis will not be required to give Customer or auditors any access or information that (i) may cause Sairis to compromise its own internal, legal, or regulatory compliance obligations, (ii) is subject to confidentiality obligations with its customers, vendors, or other third parties or (iii) is commercially sensitive (such as trade secrets).

6.5. **Third-Party Auditor**. A Third-Party Auditor means a third-party independent contractor that is not a competitor of Sairis. Upon the request by Customer for an On-Site Audit, an On-Site Audit can be conducted through a Third Party Auditor if: (i) prior to the On-Site Audit, the Third-Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Customer's Agreement to protect Sairis' proprietary information; (ii) Customer shall be jointly and severally liable with the Third-Party Auditor for any confidentiality breaches, data security incidents, or unauthorized disclosures, and Customer's indemnification obligation shall include: (a) all direct and indirect damages to Sairis and its customers; (b) costs of incident response, remediation, and regulatory notification; (c) regulatory fines, penalties, or sanctions imposed on Sairis; (d) business interruption losses and reputational damages; (e) all legal costs, expert fees, and expenses incurred by Sairis; and (f) costs of credit monitoring or other protective services for affected individuals, regardless of whether such damages were foreseeable or within Customer's control; and (iii) the costs of the Third-Party Auditor are at Customer's expense.

6.6. **Findings**. Customer must provide Sairis, via written communication, any information regarding any non-compliance discovered during the course of an On-Site Audit within three business days of the completion of an On-Site Audit. If an audit results in Sairis being notified, via written communication, that it, or its Processing of Personal Data, does not comply with Data Protection Laws, the Parties will discuss that finding and, with respect to any such non-compliance, Sairis will take corrective actions to achieve compliance to the reasonable satisfaction of the auditor and within a reasonable time frame as determined by Sairis with an obligation of corrective action within no less than 30 days from notice of non-compliance.

6.7. **Audit Redundancy**. Without prejudice to the rights granted in this Agreement, if the requested audit scope is addressed in a SOC, ISO, or similar audit report issued by a qualified third-party auditor within the prior twenty-four months, or is scheduled to be audited prior to the date of the requested audit in accordance with the written notice period in the On-Site Audit section of this agreement, and Sairis makes such report available to Customer confirming there are no known material changes in the controls audited, Customer agrees to accept the findings presented in the third-party audit report in lieu of requesting an audit of the same controls covered by the report.

6.8. **Data Protection Impact Assessment.** Upon Customer's request, Sairis shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under Data Protection Laws and Regulations 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 Sairis. Customer is responsible for any costs arising from Sairis' assistance to the extent such assistance exceeds the scope of Sairis' obligations under Data Protection Laws and/or routine customer service. If Sairis expects to incur additional costs, it will promptly inform Customer in advance, and the Parties will then negotiate in good faith to agree on such costs.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

7.1. Sairis maintains security incident management policies and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Sairis or its Sub-processors of which Sairis becomes aware (a "Customer Data Incident"). Sairis shall make reasonable efforts to identify the cause of such Customer Data Incident and take such steps as Sairis deems necessary and reasonable to remediate the cause of such a Customer Data Incident to the extent the remediation is within Sairis's reasonable control. The obligations herein shall not apply to incidents that are

caused by Customer or Customer's Users.

8. GOVERNMENT ACCESS REQUESTS

8.1. **Sairis requirements.** As a Processor, Sairis shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security. If Sairis receives a legally binding request to access Personal Data from a Public Authority, Sairis shall, unless otherwise legally prohibited, promptly notify Customer including a summary of the nature of the request. To the extent Sairis is prohibited by law from providing such notification, Sairis shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Sairis to communicate as much information as possible, as soon as possible. Further, Sairis shall challenge government requests only to the extent that such challenge can be made through commercially reasonable efforts and without subjecting Sairis to material risk of contempt of court, criminal penalties, sanctions, or other adverse legal consequences. Sairis' obligation to pursue appeals is limited to situations where legal counsel advises in writing that such appeals have reasonable prospects of success, do not expose Sairis to additional legal liability exceeding $25,000, and can be pursued without violating applicable procedural deadlines or court orders. When challenging a request, Sairis may seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. Sairis agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. Sairis shall promptly notify Customer if Sairis becomes aware of any direct access by a Public Authority to Personal Data and provide information available to Sairis in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require Sairis to pursue action or inaction that could result in civil or criminal penalty for Sairis such as contempt of court. Sairis certifies that Sairis (1) has not purposefully created back doors or similar programming for the purpose of allowing access to the Services and/or Personal Data by any Public Authority; (2) has not purposefully created or changed its business processes in a manner that facilitates access to the Services and/or Personal Data by any Public Authority; and (3) at the Effective Date is not currently aware of any national law or government policy requiring Sairis to create or maintain back doors, or to facilitate access to the Services and/or Personal Data, to keep in its possession any encryption keys or to hand-over the encryption key to any third party.

8.2. **Sub-processors requirements**. Sairis shall ensure, to the extent of its ability, that Sub-processors involved in the Processing of Personal Data are subject to the relevant commitments regarding Government Access Requests in the Standard Contractual Clauses.

9. RETURN AND DELETION OF CUSTOMER DATA

Upon termination or expiration of the Agreement and this DPA, and upon Customer's written request, Sairis will return the Personal Data and all copies to the Customer and/or will securely destroy (delete) the Personal Data and all existing copies in accordance with the Agreement, except if continued storage is required under applicable laws and permitted under Data Protection Laws. In such case, Sairis will inform the Customer of such legal obligation, keep the Personal Data confidential, and only Process the Personal Data if required by applicable laws. Until Customer Data is deleted or returned, Sairis shall continue to comply with this DPA and its Schedules.

10. AUTHORIZED AFFILIATES

10.1. **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Sairis and each such Authorized Affiliate subject to the provisions of the Agreement and this DPA. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is a party only to this DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

10.2. **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Sairis under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.3. **Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to this DPA with Sairis, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

10.3.1. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Sairis directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in section 10.3.2, below).

10.3.2. The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an On-Site Audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Sairis and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

11. LIMITATION OF LIABILITY

11.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Sairis, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Sairis' and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

11.2. **Limitation of Liability**. Neither Sairis nor any of Sairis' affiliates or licensors will be responsible to Customer for any compensation, reimbursement, or damages arising in connection with any unauthorized access to, alteration of, or the deletion, destruction, damage, loss, or failure to store any personal data. In any case, Sairis' and Sairis' affiliates' and licensors' aggregate liability under this DPA will not exceed the amount Customer already paid to Sairis under the Agreement for the Service that gave rise to the claim during the 12 months before the liability arose. The exclusions and limitations in this section apply only to the maximum extent permitted by applicable law. For the avoidance of doubt, this limitation does not apply to data subject rights provided for under applicable Data Protection Laws

12. EUROPE SPECIFIC PROVISIONS

12.1. **Definitions**. For the purposes of this section 12 and Schedule 1 these terms shall be defined as follows:

12.1.1. **"European Personal Data"** means the Personal Data subject to European Data Protection Laws and Regulations.

12.1.2. **"European Data Protection Laws and Regulations"** means the Data Protection Laws and Regulations applying in Europe.

12.1.3. **"SCC Module 2"** means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).

12.1.4. **"SCC Module 3"** means Standard Contractual Clauses sections I, II III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).

12.1.5. **"Third-Country Transfer"** means a transfer of European Personal Data that is not subject to an adequacy decision by the European Commission. When US entities part of the Sairis Group or its Sub-processors are certified under the EU-US Data Privacy Framework and its extensions, the Parties agree that transfers to such entities are not considered Third-Country Transfers.

12.2. **GDPR.** Sairis will Process Personal Data in accordance with the GDPR requirements directly applicable to Sairis' provision of its Services.

12.3. **Transfer mechanisms for data transfers.** If, in the performance or use of the Services, European Personal Data is subject to a Third-Country Transfer, the transfer mechanisms listed below shall apply:

12.3.1. **Sairis Processor BCR**, which shall apply to the Services listed in the Appendix to the Sairis Processor BCR (the "BCR Services"), subject to the additional terms in section 1 of Schedule 1;

12.3.2. **SCC Module 2.** Where Customer and/or its Authorized Affiliate is a Controller and a data exporter , subject to the additional terms in section 2 of Schedule 1; and/or

12.3.3. **SCC Module 3.** Where Customer and/or its Authorized Affiliate is a Processor acting on behalf of a Controller and a data exporter , subject to the additional terms in sections 2 and 3 of Schedule 1.

12.4. **Impact of Local Laws.** As of the Effective Date, Sairis has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the Infrastructure and Sub-processors Documentation, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent Sairis from fulfilling its obligations under this DPA. If Sairis reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("Local Laws") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Customer. In such a case, Sairis shall use reasonable efforts to make available to the affected Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Customer. If Sairis is unable to make available such change promptly, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Sairis in accordance with the Local Laws by providing written notice in accordance with the "Notices" section of the Agreement. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

13. **INDEPENDENCE TOWARDS THIRD PARTIES**

Notwithstanding provisions in this DPA related to Sairis and Sairis' responsibilities with its Sub-processors in accordance with the clauses above, for the avoidance of doubt, any third parties, including those Customer contracted with to provide consulting and/or implementation services, including third parties referred by Sairis employees or Affiliates or other Sairis communication or marketing materials, in relation to the Services, are independent of Sairis and Sairis shall in no event be responsible for their acts or omissions, including when such acts or omissions impact Customer's use of the Services.

14. **ASSIGNMENT**

Sairis may assign this DPA to an affiliate or in connection with a merger of Sairis or the sale of substantially all Sairis' assets.

15. **AMENDMENTS**

Sairis has the right, in its sole discretion, to amend this DPA from time to time for the purposes of maintaining up-to-date standards of compliance as Data Protection Laws are updated, and amended terms become effective on posting. Notwithstanding any notice provided in accordance with this DPA, Sairis may notify Customer of amendments to this DPA by posting a notification at https://www.sairis.ai/legal. Customer is responsible for reviewing any such amendments. Customer's continued use of the Software after the effective date of the amendments will be deemed acceptance of the amended terms.

16. **GOVERNING LAW**

16.1. This DPA shall only become legally binding between Customer and Sairis when the Main Services Agreement is accepted by Customer.

16.2. **Governing Law; Venue; Jurisdiction.** Without prejudice to the provisions of the EEA Standard Contractual Clauses, Swiss Addendum, and the UK Addendum addressing the law that governs them, this DPA will be governed by and construed in accordance with the laws that govern the Agreement and the venue and dispute resolution provisions under the Agreement will also apply to disputes and claims under this DPA.

16.3. **Translations.** If this Agreement is translated into languages other than English, the English version will control.

16.4. **Waiver.** Any waiver by a Party of a breach of any provision of this DPA will not operate as or be construed as a waiver of any further or subsequent breach.

16.5. **Survival.** Provisions of this DPA that by their nature are to be performed or enforced following any termination of this DPA will survive such termination.

17. **SEVERABILITY**

If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

18. **ENTIRE AGREEMENT**

This DPA constitutes the entire agreement between the Parties with respect to its subject matter and supersedes all prior understandings regarding such subject matter, whether written or oral. If a conflict exists between this DPA and the Agreement regarding the subject matter of this DPA, the terms of this DPA will govern. If a conflict exists between this DPA and the Standard Contractual Clauses regarding the subject matter of this DPA, the applicable Standard Contractual Clauses will govern.

19. **LEGAL EFFECT**

19.1. **Legal Effect.** This DPA automatically becomes legally binding between Customer and Sairis upon Customer's execution of the Main Services Agreement (MSA) or any Order Form, without requiring separate signature, execution, or specific reference in Order Forms. Customer's acceptance of the MSA constitutes full acceptance and agreement to all terms of this DPA. This DPA becomes effective as of the date Customer accepts the MSA (the "Effective Date") and applies to all Personal Data processing from that date forward. If the individual accepting the MSA is acting on behalf of a company or other legal entity, such individual represents that they have the authority to bind such entity and its affiliates to the terms of both the MSA and this DPA.

19.2. **Document Precedence for Data Processing Matters.** For matters specifically related to data processing, privacy compliance, AI processing workflows, and data protection obligations, this DPA shall take precedence over conflicting provisions in the MSA, except where the MSA provides greater protection, more favorable liability limitations, or stronger indemnification terms for Sairis, in which case the MSA provisions shall control. Standard Contractual Clauses and applicable Binding Corporate Rules shall take precedence over both this DPA and the MSA for matters within their specific scope. In case of conflicts between schedules to this DPA, the most restrictive terms favoring Sairis' protection shall apply.

20. **LIST OF SCHEDULES**

SCHEDULE 1 – Transfer Mechanisms for European Data Transfers

SCHEDULE 2 – Description of Processing/Transfer

SCHEDULE 3 – United States State-Specific Addendum

SCHEDULE 1 – TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

1. **ADDITIONAL TERMS FOR BCR SERVICES**

1.1. **Instructions and Notices.** Where Customer acts as a Processor under the instructions of the relevant Controller of Personal Data, Customer acknowledges and accepts that the commitments contained in the Sairis Processor BCR are for the benefit of the ultimate Controller. Customer shall be responsible for ensuring that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Sairis for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall also be solely responsible for forwarding any notifications received from Sairis to the relevant Controller where appropriate.

1.2. **Audits of the BCR Services.** The Parties agree that the audits of BCR Services described in the BCR shall be carried out in accordance with section 6.3 of the DPA.

1.3. **Reference to the Sairis Processor BCR.** All provisions contained in the Sairis Processor BCR, the most current versions which are available on Sairis' website, currently located at https://www.sairis.ai/legal are incorporated by reference and are an integral part of this DPA.

1.4. **Liability.** In accordance with the Agreement, Customer shall have the right to enforce the Sairis Processor BCR against the Sairis Group, including judicial remedies and the right to receive compensation.

1.5. **Conflict.** In the event of any conflict or inconsistency between this DPA and the Sairis Processor BCR, the Sairis Processor BCR shall prevail.

2. **STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS**

For the purposes of SCC Module 2 and SCC Module 3, Customer is the data exporter and Sairis LLC ("Sairis") is the data importer and the Parties agree to the following. Where the Sairis entity that is a party to this DPA is not Sairis, that Sairis entity is carrying out the obligations of the data importer on behalf of Sairis. If and to the extent an Authorized Affiliate relies on SCC Module 2 or SCC Module 3 for the transfer of Personal Data, any references to 'Customer' in this Schedule, include such Authorized Affiliate. Where this section 2 does not explicitly mention SCC Module 2 or SCC Module 3 it applies to both of them.

2.1. **Reference to the Standard Contractual Clauses.** The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.

2.2. **Docking clause.** The option under clause 7 shall not apply.

2.3. **Instructions**. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Sairis for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data are set out in section 2.2 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

2.4. **Certification of Deletion**. The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Sairis to Customer only upon Customer's written request.

2.5. **Security of Processing**. For the purposes of clause 8.6(a), Customer is responsible for making an independent determination as to whether the technical and organizational measures set forth in the Security, Privacy and Architecture Documentation meet Customer's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by Sairis provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with section 7 (Customer Data Incident Management and Notification) of this DPA.

2.6. **Audits of the SCCs**. The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with section 6.3 of this DPA.

2.7. **General authorization for use of Sub-processors**. Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Sairis has Customer's general authorization to engage Sub-processors in accordance with section 5 of this DPA. Sairis shall make available to Customer the current list of Sub-processors in accordance with section 5.2 of this DPA.

2.8. **Notification of New Sub-processors and Objection Right for new Sub-processors**. Pursuant to clause 9(a), Customer acknowledges and expressly agrees that Sairis may engage new Sub-processors as described in sections 5.2 and 5.3 of this DPA. Sairis shall inform Customer of any changes to Sub-processors following the procedure provided for in section 5.2 of this DPA.

2.9. **Complaints - Redress.** For the purposes of clause 11, and subject to section 3 of this DPA, Sairis shall inform data subjects on its website of a contact point authorized to handle complaints. Sairis shall inform Customer if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. Sairis shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer). The option under clause 11 shall not apply.

2.10. **Supervision.** Clause 13 shall apply as follows:

2.10.1. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

2.10.2. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

2.10.3. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, Commission nationale de l'informatique et des libertés (CNIL) - 3 Place de Fontenoy, 75007 Paris, France shall act as competent supervisory authority.

2.10.4. Where Customer is established in the United Kingdom or falls within the territorial scope of application of the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws and Regulations"), the Information Commissioner's Office ("ICO") shall act as competent supervisory authority.

2.10.5. Where Customer is established in Switzerland or falls within the territorial scope of application of the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws and Regulations"), the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

2.11. **Notification of Government Access Requests**. For the purposes of clause 15(1)(a), Sairis shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

2.12. **Governing Law.** The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of France; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of England and Wales.

2.13. **Choice of Forum and Jurisdiction**. The courts under clause 18 shall be those designated in the Venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) France; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the courts of England and Wales shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

2.14. **Appendix**. The Appendix shall be completed as follows:

2.14.1. The contents of section 1 of Schedule 2 shall form Annex I.A to the Standard Contractual Clauses

2.14.2. The contents of sections 2 to 9 of Schedule 2 shall form Annex I.B to the Standard Contractual Clauses

2.14.3. The contents of section 10 of Schedule 2 shall form Annex I.C to the Standard Contractual Clauses

2.14.4. The contents of section 11 of Schedule 2 to this Exhibit shall form Annex II to the Standard Contractual Clauses.

2.15. **Data Exports from the United Kingdom under the Standard Contractual Clauses**. For data transfers governed by UK Data Protection Laws and Regulations, the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18 of those Mandatory Clauses ("Approved Addendum") shall apply. The information required for Tables 1 to 3 of Part One of the Approved Addendum is set out in Schedule 2 of this DPA (as applicable). For the purposes of Table 4 of Part One of the Approved Addendum, neither party may end the Approved Addendum when it changes.

2.16. **Data Exports from Switzerland under the Standard Contractual Clauses**. For data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity. In such circumstances, general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in Swiss Data Protection Laws.

2.17. **Conflict**. The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

3. **ADDITIONAL TERMS FOR SCC MODULE 3**

For the purposes of SCC Module 3 (only), the Parties agree the following.

3.1. **Instructions and notifications.** For the purposes of clause 8.1(a), Customer hereby informs Sairis that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Customer warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Sairis for the appointment of Subprocessors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall be solely responsible for forwarding any notifications received from Sairis to the relevant Controller where appropriate.

3.2. **Security of Processing**. For the purposes of clause 8.6(c) and (d), Sairis shall provide notification of a personal data breach concerning Personal Data Processed by Sairis to Customer.

3.3. **Documentation and Compliance**. For the purposes of clause 8.9, all enquiries from the relevant Controller shall be provided to Sairis by Customer. If Sairis receives an enquiry directly from a Controller, it shall forward the enquiry to Customer and Customer shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.

3.4. **Data Subject Rights**. For the purposes of clause 10 and subject to section 3 of this DPA, Sairis shall notify Customer about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Customer shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

SCHEDULE 2 – DESCRIPTION OF PROCESSING/TRANSFER

LIST OF PARTIES

- **Data exporter(s)**: [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

  NAME:

  ADDRESS:

  CONTACT PERSON'S NAME, POSITION, AND CONTACT DETAILS:

  ACTIVITIES RELEVANT TO THE DATA TRANSFERRED UNDER THESE CLAUSES: use of Services provided by Sairis.

  SIGNATURE AND DATE:

  Role (controller/processor): Controller

- **DATA IMPORTER**:

  NAME: Sairis, LLC

  ADDRESS: 12194 S Great Plain Way, Parker, CO, 80134

  CONTACT PERSON'S NAME, POSITION, AND CONTACT DETAILS: Greg Menard, CEO

  ACTIVITIES RELEVANT TO THE DATA TRANSFERRED UNDER THESE CLAUSES: Sairis's provision of Services under the Agreement.

  SIGNATURE AND DATE:

  Role (controller/processor): Processor

1. **CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED**

1.1. Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

1.1.1. Prospects, customers, business partners and vendors of Customer (who are natural persons)
1.1.2. Employees or contact persons of Customer's prospects, customers, business partners and vendors
1.1.3. Employees, agents, advisors, freelancers of Customer (who are natural persons)
1.1.4. Customer's Users authorized by Customer to use the Services

2. **CATEGORIES OF PERSONAL DATA TRANSFERRED**

2.1. Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

2.1.1. First and last name
2.1.2. Title
2.1.3. Position
2.1.4. Employer
2.1.5. Contact information (company, email, phone, physical business address)
2.1.6. ID data
2.1.7. Professional life data
2.1.8. Personal life data
2.1.9. Localization data

3. **SENSITIVE DATA TRANSFERRED (IF APPLICABLE)**

3.1. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

3.2. Customer may at its sole discretion submit special categories of data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Customer's liability and indemnification obligations for special categories of data are governed by Section 2.5 of this DPA. Customer acknowledges that the nature of the Services provided by Sairis include opportunities for Customer and its Users of Sairis Services to upload content and data in various formats to Sairis Services outside of the intention and purposes of this DPA for use of the Services in ways within the control and sole discretion of the Customer and its Users and outside of the awareness of Sairis and its Affiliates. For the sake of clarity, special categories of data include information included in content and files uploaded to Sairis services by Customer. Customer acknowledges that at any time and at their sole discretion they may contact Sairis to pre-emptively discuss the nature of such special data and to discuss the implications of uploading such data.

4. **FREQUENCY OF THE TRANSFER**

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis depending on the use of the Services by and at the sole discretion of the Customer.

5. **NATURE OF THE PROCESSING**

The nature of the Processing is the performance of the Services pursuant to the Agreement.

6. **PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING**

Sairis will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

7. **DURATION OF PROCESSING**

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:):

7.1. As per the Sub-processor section of the DPA, the Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. Subject to the Sub-processor section of this DPA, the Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

8. **SUB-PROCESSOR TRANSFERS**

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

8.1. As per 7 above, the Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. Subject to section 9 of this DPA, the Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing. Identities of the Sub-processors used for the provision of the Services and their country of location are listed under the Infrastructure and Sub-processor Documentation, or as otherwise provided by Sairis, which can be found on Sairis' Legal webpage https://www.sairis.ai/legal.

9. **COMPETENT SUPERVISORY AUTHORITY**

9.1. Identify the competent supervisory authority/ies in accordance with clause 13: the supervisory authority specified in section 2.10 of Schedule 1 shall act as the competent supervisory authority.

10. **TECHNICAL AND ORGANIZATIONAL MEASURES**

Sairis will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security, Privacy and Architecture Documentation, or as otherwise provided by Sairis, applicable to the specific Services purchased by Customer. Sairis will not materially decrease the overall security of the Services during a subscription term.

End of Schedule 2.

SCHEDULE 3 – UNITED STATES STATE-SPECIFIC ADDENDUM

This Schedule outlines additional terms required under certain U.S. state privacy laws, including but not limited to the **California**

Consumer Privacy Act (CCPA/CPRA), the **Colorado Privacy Act (CPA)**, and the **Virginia Consumer Data Protection Act (VCDPA)**. These terms apply where and to the extent that Sairis Processes Personal Data on behalf of the Customer that is subject to these laws.

1. **DEFINITIONS**

For purposes of this Schedule, references to "Personal Data" include "personal information" as defined under applicable U.S. state laws. References to "Controller" include "Business" under CCPA/CPRA, and "Processor" includes "Service Provider" and "Contractor," as applicable under state law.

2. **RESTRICTIONS ON USE AND RETENTION**

Sairis certifies that it understands and will comply with the following restrictions:

2.1. Sairis shall not sell or share personal data (as defined under the CCPA/CPRA).

2.2. Retain, use, or disclose Personal Data for any purpose other than the business purposes specified in the Agreement and this DPA, including any internal use unrelated to the provision of the Services.

2.3. Combine Personal Data with other data unless expressly permitted by Customer or required by applicable law.

3. **CONSUMER RIGHTS ASSISTANCE**

In alignment with Section 3 of this DPA and to the extent required by applicable law, Sairis shall:

3.1. Provide reasonable assistance to Customer in responding to verifiable consumer requests to exercise privacy rights (e.g., access, deletion, correction, data portability);

3.2. Promptly notify Customer upon receiving any such request directly from a consumer and shall not respond to the request itself unless otherwise authorized in writing by Customer.

4. **SUBPROCESSOR TRANSPARENCY AND CONSENT**

Sairis shall provide advance notice of any intended changes concerning the addition or replacement of Sub-processors and shall honor Customer's right to object to such changes, as described in Section 5 of this DPA.

5. **AUDIT RIGHTS**

In compliance with applicable U.S. state privacy laws (including CPA § 6(1)(d) and VCDPA § 7.1(d)), Sairis agrees to audits as outlined in Section 6.3 of this DPA, allowing Customer to verify Sairis' compliance with its obligations as a Processor or Service Provider.

6. **NO CROSS-CONTEXT BEHAVIORAL ADVERTISING**

Sairis shall not Process Personal Data for purposes of **targeted advertising** or **cross-context behavioral advertising** as defined under applicable state privacy laws, unless explicitly instructed by Customer and permitted under the Agreement.

7. **JURISDICTION-SPECIFIC CERTIFICATIONS**

7.1. Sairis certifies that it will act as a Service Provider under CCPA/CPRA.

7.2. Sairis certifies that it will act as a Processor under CPA and VCDPA

7.3. Sairis certifies that it will comply with all applicable obligations imposed on Processors and Service Providers under these

laws.

8. **CONFLICTS**

In the event of any conflict between this Schedule and the rest of the DPA, this Schedule shall control only to the extent required by applicable U.S. state privacy law.

End of Schedule 3.