

Addendum to Sayari Master Services Agreement: Data Processing Agreement

This Data Processing Addendum (“**Addendum**”) forms part of the Contract for Services (“**Agreement**”) between the Customer identified in the related Agreement (the “**Customer**”) and Sayari Labs, Inc. (“**Sayari**”) (Sayari and the Customer, each a Party and together the “**Parties**”) and applies to Sayari’s processing of personal data provided or made available by the Customer and/or its affiliates to Sayari in connection with the Agreement.

- 1 Any capitalized term used but not defined in this Addendum shall have the meanings ascribed to such terms in the Agreement, and for the purpose of this Addendum, the terms “**controller**”, “**processor**”, “**business**”, “**service provider**”, “**data subject**”, “**supervisory authority**” and “**processing**” shall have the meanings given in the Data Protection Laws and “**process**” and “**processed**” shall be construed accordingly.

“**Data Protection Laws**” means all applicable laws and regulations relating to privacy or the protection or processing of personal data, including without limitation, to the extent applicable: the General Data Protection Regulation (Regulation (EU) 2016/679) (“**EU GDPR**”), the EU GDPR as it forms part of the laws of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union Withdrawal Act 2018 (“**UK GDPR**”), the e-Privacy Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003, the UK Data Protection Act 2018, and including in respect of the foregoing any implementing or successor legislation and any amendments or re-enactments; the Swiss Federal Act on Data Protection (“**FADP**”); and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., including its regulations and the amendments made by the California Privacy Rights Act of 2020 (“**CCPA**”), the Virginia Consumer Data Protection Act (“**VCDPA**”), the Colorado Privacy Act and related regulations (“**CPA**”), and any other similar state law governing the Processing of Personal Data (collectively, “**U.S. State Privacy Laws**”). For the avoidance of doubt, if the Parties’ Processing activities involving Personal Data are not within the scope of a given Data Protection Law, such law is not applicable for purposes of this Addendum.

“**Personal Data**” refers to any information relating to an identified or identifiable natural person that Sayari Processes on behalf of Customer under the Agreement. For purposes of this ADDENDUM, the term “Personal Data” includes “personal information,” “personally identifiable information,” and similar terms defined under Data Protection Laws, but does not include Business Contact Information or Usage Data, as such terms are defined in the Agreement.

“**Personal Data Breach**” means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data occurring on Sayari's systems or otherwise under Sayari's control.

“Standard Contractual Clauses” means the European Commission’s Standard Contractual Clauses for the transfer of personal data from the European Union to processors established in third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to the European Commission’s Implementing Decision (EU) 2021/914 located http://data.europa.eu/eli/dec_impl/2021/914/oj and executed by and between the Customer and Sayari pursuant to the Agreement, and completed as set forth in Section 6 below.

“UK Approved Addendum” means, to the extent applicable, Template Addendum B.1.0 issued by the UK ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (available as of the Effective Date at <https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf>).

- 2 The Parties acknowledge and agree that for the purposes of the Data Protection Laws, the Customer is the controller, and Sayari is the processor, in relation to the processing set out below:
 - 2.1 *scope, nature and purpose of processing*: processing carried out by Sayari in the provision of the Services;
 - 2.2 *duration*: for the Term; and
 - 2.3 *types of personal data and categories of data subjects*: data subjects whose personal data is processed by Sayari in performance of the Services.
- 3 The Customer shall comply with all applicable Data Protection Laws, including those regarding the legality of collection, quality and accuracy of personal data that is transferred to and processed by Sayari pursuant to the terms of the Agreement and/or this Addendum.
- 4 In processing personal data on behalf of the Customer during the provision of the Services, Sayari (acting as processor) shall:
 - 4.1 only process personal data in accordance with applicable Data Protection Laws and the instructions of the Customer as set out in the Agreement;
 - 4.2 not “sell” personal data (as such term in quotation marks is defined in applicable Data Protection Laws), “share” or process personal data for purposes of “cross-context behavioral advertising” or “targeted advertising” (as such terms in quotation marks are defined in applicable Data Protection Laws), or otherwise process personal data for any purpose other than for the specific purposes set forth herein or outside of the direct business relationship with Customer. For the avoidance of doubt, Sayari will process personal data solely to provide the corporate risk intelligence services to Customer as set forth in the Agreement, or as otherwise permitted by Data Protection Laws (for example, to comply with Sayari’s legal obligations);
 - 4.3 comply with any applicable restrictions under Data Protection Laws on combining the Personal Data with personal data that Sayari receives from, or on behalf of, another person or persons, or that Sayari collects from any interaction between it and any Data Subject;
 - 4.4 provide the same level of protection for the personal data as is required under Data Protection Laws applicable to Customer;
 - 4.5 take appropriate technical and organisational measures to protect such personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing;

- 4.6 ensure any person that Sayari discloses such personal data to have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in respect of such personal data;
- 4.7 provide reasonable cooperation as requested by the Customer to assist the Customer with (i) responding to any verifiable request from a data subject (or their lawful representative) to exercise the data subject's rights under Data Protection Laws and, (ii) at Customer's reasonable expense, fulfilling Customer's obligation to conduct a data protection impact assessment of processing or proposed processing of personal data, when required by applicable Data Protection Laws;
- 4.8 provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory and supervisory authorities in relation to the processing or proposed processing of personal data, and notify Customer of (i) any third-party complaints regarding the processing of personal data; or (ii) any government requests for access to or information about Sayari's processing of personal data on Customer's behalf, unless prohibited by Data Protection Laws. Sayari will provide Customer with reasonable cooperation and assistance in relation to any such request. If Sayari is prohibited by applicable Data Protection Laws from disclosing the details of a government request to Customer, Sayari shall inform Customer that it can no longer comply with Customer's instructions under this Addendum without providing more details;
- 4.9 notify Customer if Sayari determines that (i) it can no longer meet its obligations under this Addendum or applicable Data Protection Laws; or (ii) in its opinion, an instruction from Customer infringes applicable Data Protection Laws.
- 4.10 upon the termination or expiry of the Agreement for any reason, delete, or return to the Customer, all such personal data as soon as reasonably practicable, unless it is necessary for Sayari or its sub-contractors to retain certain copies of such personal data to comply with any applicable laws or to comply with their obligations under the Agreement;
- 4.11 by entering into this Addendum, certify it understands its obligations under this Addendum (including without limitation the restrictions under Sections 3 and 4) and that it will comply with them.

5 Sub-processors.

- 5.1 Customer acknowledges and agrees that Sayari may use Sayari affiliates and other sub-processors to process personal data in accordance with the provisions within this Addendum and Data Protection Laws. Where Sayari sub-contracts any of its rights or obligations concerning personal data, including to any affiliate, Sayari will take steps to select and retain sub-processors that are capable of maintaining appropriate privacy and security measures to protect personal data consistent with applicable Data Protection Laws and require that each sub-processor complies with obligations that are no less restrictive than those imposed on Sayari under this Addendum.
- 5.2 The Customer hereby provides Sayari with authorisation to use any of the sub-processors (as applicable) listed at <https://sayari.com/subprocessors>. Sayari may, at its sole discretion and at any time, add or remove sub-processors from this list and provided that the Customer does not object to such changes (acting reasonably and in good faith) within [ten (10) days] of such change the relevant sub-processor shall be deemed accepted by the Customer. If the Customer objects to a sub-processor, Sayari shall: (i) refrain from using such sub-processor in the context of the processing of personal data subject to the terms of this Addendum; or (ii) make available a change in the Services or recommend a change to the configuration or use of the Services to avoid the processing of personal data by the objected-to sub-processor. If Sayari is unable to make available such change within a reasonable period of time, which shall not

exceed ninety (90) days, Sayari may, by providing written notice, terminate the Service which cannot be provided without the use of the objected-to sub-processor by providing written notice.

6 Data transfers.

- 6.1 Where Sayari transfers personal data to any recipient not covered by a framework recognised by the applicable Data Protection Laws as providing an adequate level of protection for personal data (a “**Third Country**”), Sayari shall ensure that such transfer of personal data complies with applicable Data Protection Laws. Where Sayari engages in an onward transfer of personal data, Sayari shall ensure that a lawful data transfer mechanism is in place prior to transferring personal data from one country to another.
- 6.2 To the extent that the Customer transfers personal data to, or otherwise makes available personal data in, a Third Country from: (i) the EEA, Module Two of the Standard Contractual Clauses shall apply to Sayari’s processing of such personal data; and/or (ii) the UK, the UK Approved Addendum shall apply alongside the Standard Contractual Clauses.
- 6.3 To the extent legally required, by signing this Addendum, Customer and Sayari are deemed to have signed the Standard Contractual Clauses, which form part of this Addendum and (except as described in Sections 6.4 and 6.5 below) shall be deemed completed as follows:
 - 6.3.1 Clause 7 (Docking Clause) shall apply;
 - 6.3.2 Option 1 of Clause 9 shall be deleted and Option 2 shall apply. The initial list of sub-processors is set forth in Schedule 2 of this Addendum and the relevant time period is 10 days;
 - 6.3.3 The option in Clause 11(a) (Redress) shall not apply;
 - 6.3.4 The governing law under Clause 17 shall be that of the Republic of Ireland and the forum under Clause 18 shall be the courts of the Republic of Ireland;
 - 6.3.5 Annex I, Parts A and B (*List of parties*) is completed as set forth in Schedule 1 of this Addendum;
 - 6.3.6 Annex I, Part C (*Competent Supervisory Authority*) of the Standard Contractual Clauses is hereby deemed to be completed with reference to the Irish Data Protection Commission;
 - 6.3.7 Annex II of the Standard Contractual Clauses (*Technical and organisational measures including technical and organisational measures to ensure the security of the data*) is hereby deemed to be completed by reference to Schedule 1 of this Addendum; and
 - 6.3.8 Annex III of the Standard Contractual Clauses (*List of Sub-processors*) is not applicable as the Parties have chosen General Authorization under Clause 9. However, a list of Sayari’s sub-processors is available in Schedule 2.
- 6.4 With respect to personal data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction or Switzerland) governs the international nature of the transfer, the UK Approved Addendum forms part of this Addendum and takes precedence over the rest of this Addendum as set forth in the UK Approved Addendum. Undefined capitalized terms used in this provision shall mean the definitions in the UK Approved Addendum. The UK Approved Addendum shall be deemed completed as follows:

- 6.4.1 Table 1. The “start date” will be the date the Agreement enters into force. The “Parties” are the Customer as exporter and Sayari as importer.
 - 6.4.2 Table 2. Module Two of the Standard Contractual Clauses applies.
 - 6.4.3 Table 3. The “Appendix Information” is the information set out in Clause 6.3 of this Addendum, and as set forth in Schedules 1 and 2 below.
 - 6.4.4 Table 4. Either party may end the UK Approved Addendum in accordance with its Section 19.
 - 6.5 For transfers of personal data that are subject to the FADP, the Standard Contractual Clauses form part of this Addendum as set forth in Section 7(b) of this Addendum, but with the following differences to the extent required by the FADP: (i) references to the GDPR in the Standard Contractual Clauses are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (ii) references to personal data in the Standard Contractual Clauses also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; (iii) the term “member state” in the Standard Contractual Clauses shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses; and (iv) the relevant supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the Standard Contractual Clauses (where the FADP and GDPR apply, respectively).
 - 6.6 To the extent necessary to comply with applicable Data Protection Laws, the Parties agree to execute such additional documents (including updates to the Annexes of the Standard Contractual Clauses) and apply additional protections, as may be necessary for the transfer and storage of personal data transferred pursuant to the Standard Contractual Clauses, UK Approved Addendum, or other applicable lawful transfer mechanisms.
- 7 Personal data breach.
- 7.1 Sayari shall notify the Customer without undue delay upon Sayari becoming aware of a personal data breach affecting personal data provided by or made available by the Customer which is subject to this Addendum. Sayari will comply with the Personal Data Breach-related obligations directly applicable to it under Data Protection Laws and will provide reasonable assistance to Customer in Customer’s compliance with its Personal Data Breach-related obligations, including without limitation by:
 - 7.1.1 Taking commercially reasonable steps to mitigate the effects of the Personal Data Breach and reduce the risk to data subjects whose personal data was involved; and
 - 7.1.2 Providing Customer with the following information, to the extent available to Sayari: (a) the nature of the breach, including the categories and approximate number of data subjects and records concerned; (b) the contact at Sayari who will liaise with the Customer concerning the breach; and (c) the remediation measures being taken to mitigate and contain the breach.
- 8 Audits. To the extent required by applicable Data Protection Law, upon thirty (30) days advance written notice, Sayari shall make available all information necessary for Customer to confirm Sayari’s compliance with this Addendum. If Customer has a reasonable basis to conclude that such information provided by Sayari is not satisfactory to confirm such compliance, Customer may, at Customer’s sole expense, upon reasonable prior notice, and subject to any confidentiality or security requirements reasonably requested by Sayari, conduct an audit during normal business hours and in a manner that

does not disrupt Sayari's business of those Sayari systems and records relevant to Sayari's processing of personal data on Customer's behalf. Customer shall limit its exercise of audit rights to not more than once in any twelve (12) calendar month period, unless (i) required by instruction of a regulatory or supervisory authority; or (ii) following a Personal Data Breach. Notwithstanding the foregoing, Sayari shall have the right to limit or exclude Customer's access to Sayari proprietary systems, trade secrets, or sensitive operational data, other than where required by order of court or regulatory body.

- 9 The terms and conditions included in this Addendum shall supersede and replace any and all prior data protection agreements or prior versions of the Standard Contractual Clauses or data privacy or data protection terms included in any other agreements between the Parties relating to the subject-matter covered by this Addendum.

Schedule 1

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The exporter (Controller) is Customer and Customer's contact details and signature are as provided in the Agreement and the Addendum.

Data importer(s): The importer (Processor) is Sayari and Sayari's contact details and signature are as provided in the Agreement and the Addendum.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: The Personal Data transferred concerns data subjects whose information Customer makes available through its use of the services under the Agreement.

Categories of personal data transferred: Any personal data provided by Customer to Sayari for Sayari to perform services under the Agreement.

Sensitive data transferred (if applicable): N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): On a continuous basis as needed to provide the services to Customer.

Nature of the processing: The nature of the Processing is set out in the Agreement between the Parties.

Purpose(s) of the data transfer and further processing: The purpose of the data transfer is to provide the services chosen by Customer in connection with the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: The data will be retained for the time period needed to accomplish the purposes of Processing, unless otherwise required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: Same as above to the extent that Personal Data is provided to sub-processors for purposes of providing the services under the Agreement to Customer.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: The data exporter's competent supervisory authority will be determined in accordance with the GDPR, and where possible, will be the Irish Data Protection Commissioner.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Sayari has established and documented IT security policies and procedures, which includes technical and organisational measures such as:

- o **Encryption.** Data at rest is protected with AES-256 encryption, while data in transit uses TLS 1.2+. Encryption keys are securely managed via Google Cloud Platform and Amazon Web Services and are accessible only to a limited number of staff. All devices accessing customer data are protected with full disk encryption.
- o **Physical Access Control.** Data is securely hosted in Google Cloud Platform and AWS GovCloud data centers. These facilities boast advanced physical security measures, including badge readers, biometric identification, security guards, CCTV, and alarmed exits. Access for visitors is strictly controlled, requiring

ID verification and an escort, with all visits logged and reviewed. Only authorized personnel are granted access, and all access procedures are thoroughly documented.

- o **Network Security.** Network security measures such as firewall, router security, remote access controls, detection of unauthorized or malicious network activity via anti-virus applications, and conducting vulnerability identification and testing.
- o **Logging and Log Management Controls.** Centralized logging system captures and stores event logs for user activities, exceptions, faults, and information security events. A SIEM solution unifies logs for incident investigations, and automated alerts notify IT management of suspicious activities. Audit logs are also maintained and reviewed as needed.
- o **Technical Vulnerability Management and Protection from Malware.** An established vulnerability management process that is documented and regularly reviewed based on business and information security requirements.
- o **Data Access Control.** Access authorization and data access rights are granted on a need-to-know basis and to ensure that only persons authorized to use data processing procedures have access to personal data subject to their right of access, as well as monitoring and tracking access.
- o **Documentation Retention and Disposal.** Measures to ensure that data is regularly backed-up, stored for only as long as required for legal, regulatory and business requirements and once such data is no longer needed it is disposed of through approved methods.

In each case, at a standard that offers the personal data that Sayari processes on behalf of the Customer, the same level of protection as Sayari applies to its own personal data.

Schedule 2

SAYARI SUBPROCESSORS

The Parties agree that the sub-processors, currently listed at <https://sayari.com/subprocessors/>, are approved.