DATA PROCESSING AGREEMENT

July 2026

1. GENERAL

1.1 This data processing agreement (the "Data Processing Agreement") governs Secretariat Advisors, LLC's Processing of Personal Data as part of Vendor's provision of services ("Services") to a client ("You" or "Your"). The Services are described in the contract by which the Client engaged Services from Vendor (the "Contract").

1.2 Unless otherwise stated in the Contract, this Data Processing Agreement is incorporated into and subject to the terms of the Contract and shall be effective and remain in force for the term of the Services.

1.3 Except as stated otherwise in this Data Processing Agreement, in the event of any conflict between the terms of the Contract, including any attachments or exhibits referenced therein, and the terms of this Data Processing Agreement, the relevant terms of this Data Processing Agreement shall take precedence.

2. DEFINITIONS

2.1 "Vendor" means Secretariat Advisors, LLC;

2.2 "Vendor Affiliate(s)" means any entity which Vendor directly or indirectly controls or is controlled by or is under joint control with Vendor, that may assist in the performance of the Services as set forth in Section 3.3;

2.3 "Applicable Data Protection Law" means all applicable federal, state, and foreign laws and regulations governing the Processing of the Personal Data under this Data Processing Agreement;

2.4 "Binding Corporate Rules" has the meaning set forth under Applicable Data Protection Law;

2.5 "Controller" means any person or entity which determines the purposes and means of the processing, including, as applicable, any "business", as that term is defined by Applicable Data Protection Laws.

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

2.7 "EU Model Clauses" means the standard contractual clauses annexed to the EU Commission Decision (EU) 2021/914 of 4 June 2021 for the Transfer of Personal Data to Processors established in Third Countries under the Directive 95/46/EC, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision;

2.8 "Personal Data" means (a) information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular natural person or household; or (b) any information defined as "personal data", "personal information," or other similar terms under Applicable Data Protection Laws that Vendor Processes on Your behalf as

part of the Services. For clarity, Vendor is a Processor with respect to Personal Data that You provide to Vendor for Processing in order to provide the Services to You.

2.9 "Personal Data Breach" means the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, or access to, Your Personal Data transmitted, stored or otherwise Processed by Vendor or any Subprocessor.

2.10 "Process/Processing" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available.

2.11 "Processor" means any person or entity which Processes Personal Data, including, as applicable, any "service provider" or "contractor", as those terms are defined by Applicable Data Protection Laws.

2.12 "Regulator" means any independent public authority, government agency, and any similar regulatory authority responsible for the enforcement of Data Protection Laws.

2.13 "Third Party Subprocessor" means a third party subcontractor, other than a Vendor Affiliate, engaged by Vendor and which may Process Personal Data.

2.14 "UK Addendum" means the international data transfer addendum, issued under Section 119A of the Data Protection Act 2018, to the EU Model Clauses for international data transfers. Other capitalized terms have the definitions provided for them in the Contract, Applicable Data Protection Law, or as otherwise specified below.

2.15 "Deidentified Information" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular Data Subject.

3. PROCESSING

3.1 You are the Controller of the Personal Data provided by You to Vendor for Processing. You must comply with Your obligations under Applicable Data Protection Law, including but not limited to: (a) validly transmitting Personal Data to Vendor; (b) providing any notices to, or obtaining consent from, any Data Subjects; (c) securing a permissible legal purpose for Processing; and (d) Your other decisions and actions concerning the Processing of Personal Data.

3.2 Vendor is a Processor of the Personal Data provided by You to Vendor for Processing as part of the Services provided to You as specified in the Contract. However, Vendor is a Controller of Personal Data that you do NOT provide to Vendor for Processing as part of the Services provided to You as specified in the Contract (e.g. Vendor's client relationship data that may pertain to You). Vendor is responsible for compliance with its obligations under this Data Processing Agreement and with its obligations as a Processor under Applicable Data Protection Laws.

3.3 Vendor and any persons acting under the authority of Vendor, including any Vendor Affiliates and Third Party Subprocessors identified at www.secretariat-intl.com/third-party-processors, will Process

Personal Data solely for the purpose of (i) providing the Services in accordance with the Contract and this Data Processing Agreement, (ii) improving the Services within the scope of what is permitted of Processors by Applicable Data Protection Laws, (iii) complying with Your written instructions, or (iv) complying with Vendor's legal and regulatory obligations.

3.4 You are providing Personal Data to Vendor for the limited and specified purpose of facilitating Vendor's provision of the Services to You as further specified in Exhibit 1. Vendor will not (i) retain, use, or disclose Your Personal Data for any purpose other than the business purposes specified in the contract or as otherwise permitted by Applicable Data Protection Law, (ii) retain, use, or disclose Your Personal Data outside the direct business relationship with You, unless expressly permitted by Applicable Data Protection Law (iii) share or sell (as those terms are defined by Applicable Data Protection Law) Your Personal Data, (iv) share or sell Your Personal Data for the purpose of cross-context behavioral advertising, or (v) combine Your Personal Data with personal data Vendor receives from or on behalf of another client, except for the purpose of performing (a) Vendor's obligations to You under this Data Processing Agreement, the Contract, and any additional written instructions provided by You or (b) Vendor's obligations under applicable law. You may, at any time, provide written instructions, or, upon advanced notice to Vendor, take reasonable and appropriate steps, to stop and/or remediate the unauthorized use of Your Personal Data.

3.5 Vendor (i) shall comply with all obligations and restrictions imposed on it by Applicable Data Protection Laws in its role as a Processor, including providing the same level of privacy protection as required by Applicable Data Protection Laws; and (ii) shall notify You if Vendor determines that it can no longer meet its obligations under Applicable Data Protection Laws.

3.6 If Vendor receives Deidentified Information from You, or creates Deidentified Information at Your instruction, Service Provider will (a) take reasonable measures to ensure the Deidentified Information cannot be associated with a Data Subject or household, (b) publicly commit to maintain and use the Deidentified Information in deidentified form, and (c) not attempt to reidentify the Deidentified Information except for the sole purpose of determining whether Your deidentification processes satisfy the requirements of Applicable Data Protection Laws.

3.7 Vendor may use artificial intelligence tools to provide the Services to You, within the scope of what is permitted of Processors by Applicable Data Protection Laws and the Data Processing Agreement. For additional information, please review Vendor's "Responsible Use of Artificial Intelligence" disclosure available at http://www.secretariat-intl.com/responsible-ai.

4. CATEGORIES OF PERSONAL DATA AND DATA SUBJECTS

4.1 The subject-matter of the Processing, 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 Data Processing Agreement are further specified in Exhibit 1 attached hereto.

4.2 Unless otherwise specified in the Contract, Personal Data Processed may not include any sensitive or special personal data that imposes specific data security or data protection obligations on Vendor in addition to or different from those specified herein.

5. YOUR INSTRUCTIONS

5.1 Vendor will Process Personal Data on Your written instructions as specified in the Contract and this Data Processing Agreement, including instructions regarding data transfers as set forth in Section 7.

5.2 You may provide additional instructions in writing to Vendor with regard to Processing of Personal Data in accordance with Applicable Data Protection Law. Vendor will comply with all such reasonable instructions to the extent necessary for Vendor to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Services, including assistance with notifying individuals of Personal Data breaches as set forth in Section 11, Data Subject requests as set forth in Section 6, and data protection impact assessments (DPIAs).

5.3 To the extent required by Applicable Data Protection Law, Vendor will inform You if, in its opinion, Your instruction infringes Applicable Data Protection Law. You acknowledge and agree that Vendor is not responsible for performing legal research and/or for providing legal advice to You concerning the Processing of Your Personal Data or any other matter.

5.4 Without prejudice to Vendor's obligations under this Section 5, You agree to pay reasonable charges that may be incurred by Vendor to comply with instructions with regard to the Processing of Personal Data that require the use of resources different from or in addition to those required for the provision of the Services.

6. RIGHTS OF DATA SUBJECTS

6.1 If possible, Vendor will grant You electronic access to Your Personal Data to enable You to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law, including requests to access, delete or erase, restrict, rectify, receive and transmit, block access to or object to Processing of specific Personal Data or sets of Personal Data.

6.2 You can provide detailed written instructions to Vendor (including the Personal Data necessary to identify the Data Subject) on how to assist with such Data Subject requests in relation to Personal Data. Vendor will promptly follow such instructions. If applicable, the parties will negotiate in good faith with respect to any charges or fees that may be incurred by Vendor to comply with instructions that require the use of resources different from or in addition to those required for the provision of the Services.

6.3 If Vendor directly receives any Data Subject requests regarding Personal Data, it will pass on such requests to You without responding to the Data Subject, if the Data Subject identifies You as the Data Controller. If the Data Subject does not identify You, Vendor will instruct the Data Subject to contact the entity responsible for collecting their Personal Data.

7. PERSONAL DATA TRANSFERS

7.1 Vendor may access and Process Personal Data on a global basis as necessary to perform the Services, including for IT security purposes, maintenance and related infrastructure, technical support

and change management.

7.2 To the extent such global access involves a transfer of Personal Data originating from the European Economic Area ("EEA"), Switzerland or the UK to Vendor Affiliates or Third Party Subprocessors located in countries outside the EEA, Switzerland or the UK that have not received a binding adequacy decision by the European Commission or by a competent national EEA, Swiss or UK data protection authority, such transfers are subject to (i) the terms of the EU Model Clauses, or UK Addendum, as applicable, both of which are incorporated into this Data Processing Agreement by reference, specifically, Module 2 where You are the Controller and Vendor is a Processor ; or (ii) other binding and appropriate transfer mechanisms that provide an adequate level of protection in compliance with Applicable Data Protection Law, such as approved Binding Corporate Rules for Processors. To the extent such global access involves the onward transfer of Personal Data originating from the European Economic Area ("EEA"), Switzerland or the UK to a Third Party Subprocessor that is both (a) locatedin the United States and (b) is an active participant in the Data Privacy Framework as set forth by the United States Department of Commerce, including applicable Switzerland and UK extensions (collectively, "DPF"), Vendor may choose to rely on the DPF for such onward transfers. For the purposes of the EU Model Clauses and UK Addendum, You and Vendor agree that (i) You will act as the data exporter on Your own behalf and on behalf of any of Your entities, (ii) Vendor will act on its own behalf and/or on behalf of the relevant Vendor Affiliates as the data importers, (iii) any Third Party Subprocessors will act as 'subcontractors' pursuant to Clause 11 of the EU Model Clauses and UK Addendum.

7.3 Transfers of Personal Data originating from other locations globally to Vendor Affiliates or Third Party Subprocessors are subject to (i) for Vendor Affiliates, the terms of the Vendor Intra-Company Data Processing and Transfer Agreement entered into between the relevant Vendor entities, which requires all transfers of Personal Data to be made in compliance with all applicable Vendor security and data privacy policies and standards; and (ii) for Third Party Subprocessors, the terms of the relevant Vendor Third Party Subprocessor agreement incorporating security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement.

7.4 For the purposes of the EU Model Clauses:

- Clause 9(a), Module 2: the parties select Option 2. The time period is 14 calendar days.
- Clause 11(a): the parties do not select the independent dispute resolution option.
- Clause 17, Module 2 and: the parties select Option 2. The Member State of the data exporter is Ireland.
- Clause 18(b), Module 2: the Parties agree that those shall be the courts of Ireland.
- Annex I(A): You are the data exporter. Vendor is the data importer. Your contact details are set forth in the Contract. Contact details for Vendor are: legal@secretariat-intl.com.
- Annex I(B): the parties agree that the information regarding transfer is set forth in Vendor's privacy policy and within this Data Processing Agreement.
- Annex I(C): the competent supervisory authority is the supervisory authority in the EU Member State where You or Your EU data representative are located.
- Annex II: the parties agree that Section 9 describes the technical and organizational measures applicable to the transfer.

7.5 The terms of this Data Processing Agreement shall be read in conjunction with the EU Model Clauses, UK Addendum, and other applicable transfer mechanisms pursuant to this Section 7. To the extent there is any conflict between this Data Processing Agreement and the EU Model Clauses or the UK Addendum, the EU Model Clauses or UK Addendum shall prevail.

8. VENDOR AFFILIATES AND THIRD PARTY SUBPROCESSORS

8.1 Subject to the terms and restrictions specified in Sections 3.3, 7 and 8, You agree that Vendor may engage Vendor Affiliates and Third Party Subprocessors to assist in the performance of the Services.

8.2 Vendor maintains lists of Vendor Affiliates and Third Party Subprocessors that may Process Personal Data. These lists are available at www.secretariat-intl.com/third-party-processors.

8.3 Vendor will post changes in its Vendor Affiliates and Third Party Subprocessors by updating the information posted at www.secretariat-intl.com/third-party-processors. Vendor shall notify You if it adds, removes, or substitutes any Vendor Affiliates or Third Party Subprocessors if You opt-in to receiving such notifications by providing Your contact information. You can opt-out of receiving such notifications by following the instructions here. You should monitor the list of Vendor Affiliates and Third Party Subprocessors frequently for changes, as Vendor's updating of the list constitutes notice to You. Within fourteen (14) calendar days of Vendor providing notice or posting any such changes, You may object to the intended involvement of a Third Party Subprocessor or Vendor Affiliate in the performance of the Services, providing objective justifiable grounds related to the ability of such Third Party Subprocessor or Vendor Affiliate to adequately protect Personal Data in accordance with this Data Processing Agreement or Applicable Data Protection Law, in writing through Vendor's primary support channel. In the event Your objection is justified, You and Vendor will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Subprocessors' or Vendor Affiliate's compliance with this Data Processing Agreement or Applicable Data Protection Law, or delivering the Services without the involvement of such Third Party Subprocessor. To the extent You and Vendor do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Services (i) upon serving prior notice in accordance with the terms of the Contract; (ii) without liability to You and Vendor; and (iii) without relieving You from Your payment obligations under the Contract.

8.4 The Vendor Affiliates and Third Party Subprocessors are required to abide by the terms of this Data Processing Agreement, and the level of data protection and security under Applicable Data Protection Law.

8.5 Vendor remains responsible at all times for the performance of the Vendor Affiliates' and Third Party Subprocessors obligations in compliance with the terms of this Data Processing Agreement and Applicable Data Protection Law.

9. TECHNICAL AND ORGANIZATIONAL MEASURES, AND CONFIDENTIALITY OF PROCESSING

9.1 Vendor has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data. Such measures shall include the measures described

in Exhibit 2 of this Data Processing Agreement (the "Security Measures"). The Security Measures take into account the nature, scope and purposes of Processing as specified in this Data Processing Agreement and are intended to protect Personal Data against the risks inherent to the Processing of Personal Data in the performance of the Services, in particular risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

9.2 In particular, the Security Measures include physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. You are advised to ensure that the Security Measures and other practices are appropriate for the Processing of Personal Data pursuant to this Data Processing Agreement.

9.3 All Vendor and Vendor Affiliate staff, as well as any Third Party Subprocessors that may have access to Personal Data are subject to appropriate confidentiality arrangements.

10. AUDIT RIGHTS AND COOPERATION WITH YOU AND YOUR REGULATORS

10.1 You may audit Vendor's compliance with its obligations under this Data Processing Agreement up to once per year. In addition, to the extent required by Applicable Data Protection Law, including where mandated by Your Regulator, You or Your Regulator may perform more frequent audits. Vendor will contribute to such audits by providing You or Your Regulator with the information and assistance reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the Services ordered by You.

10.2 If a third party is to conduct the audit, the third party must be mutually agreed to by You and Vendor (except if such third party is a competent Regulator). The third party must execute a written confidentiality agreement acceptable to Vendor or otherwise be bound by a statutory confidentiality obligation before conducting the audit.

10.3 To request an audit, You must submit a detailed proposed audit plan to Vendor at least thirty (30) days in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Vendor will review the proposed audit plan and provide You with any concerns or questions (for example, any request for information that could compromise Vendor's security, privacy, employment or other relevant policies). Vendor will work cooperatively with You to agree on a final audit plan. The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Vendor's health and safety or other relevant policies, and may not unreasonably interfere with Vendor's business activities.

10.4 If the requested audit scope is addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve (12) months and Vendor provides such report to You confirming there are no known material changes in the controls audited, You agree 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.

10.5 You will provide Vendor any audit reports generated in connection with any audit under this Section 10, unless prohibited by Applicable Data Protection Law or otherwise instructed by a Regulator. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement. The audit reports are Confidential Information of the parties under the terms of the Contract.

10.6 Any audits are at Your expense. You will pay any reasonable charges or fees that may be incurred by Vendor to provide assistance with an audit that requires the use of resources different from or in addition to those required for the provision of the Services.

11. INCIDENT MANAGEMENT AND PERSONAL DATA BREACH NOTIFICATION

11.1 Vendor promptly evaluates and responds to incidents that create suspicion of or indicate potential unauthorized access to or Processing of Personal Data ("Incident"). All Vendor and Vendor Affiliates staff that have access to or Process Personal Data are instructed on responding to Incidents, including prompt internal reporting, escalation procedures, and chain of custody practices to secure relevant evidence. Third Party Subprocessors are expected to meet their Incident reporting obligations under Applicable Data Protection Law.

11.2 In order to address an Incident, Vendor defines escalation paths and response teams involving internal functions such as Information Security and Legal. The goal of Vendor's Incident response will be to restore the confidentiality, integrity, and availability of the Services environment and the Personal Data that may be contained therein, and to establish root causes and remediation steps. Depending on the nature and scope of the Incident, Vendor may also involve and work with You and outside law enforcement to respond to the Incident.

11.3 To the extent Vendor becomes aware of a confirmed Personal Data Breach, Vendor will inform You of such Personal Data Breach without undue delay.

11.4 Vendor will take reasonable measures designed to identify the root cause(s) of the Personal Data Breach, mitigate any possible adverse effects and prevent a recurrence. As information regarding the Personal Data Breach is collected or otherwise reasonably becomes available to Vendor and to the extent permitted by law, Vendor will provide You with (i) a description of the nature and reasonably anticipated consequences of the Personal Data Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; (iii) where possible, the categories of Personal Data and Data Subjects including an approximate number of Personal Data records and Data Subjects that were the subject of the Personal Data Breach; and (iv) other information concerning the Personal Data Breach reasonably known or available to Vendor that You may be required to disclose to a Regulator or affected Data Subject(s).

11.5 Unless otherwise required under Applicable Data Protection Law, the parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant Regulators.

11.6 Vendor will cooperate, and require any Subprocessor to cooperate, with You in the investigation, mitigation, and remediation of any such Personal Data Breach.

12. RETURN AND DELETION OF PERSONAL DATA UPON TERMINATION OF SERVICES

12.1 You are advised to take appropriate action to back up or otherwise store separately any Personal Data prior to the termination of the Services. You may make a written request to Vendor for the retrieval of, or access to, Your Personal Data up to ten (10) days prior to the termination of Services.

12.2 Upon termination of the Services, Vendor will promptly delete all copies of Personal Data from the Services environment by rendering such Personal Data unrecoverable, except as may be required by law.

13. LEGALLY REQUIRED DISCLOSURE REQUESTS

13.1 If Vendor receives any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority which relates to the Processing of Personal Data ("Disclosure Request"), it will promptly pass on such Disclosure Request to You without responding to it, unless otherwise required by applicable law (including to provide an acknowledgement of receipt to the authority that made the Disclosure Request).

13.2 At Your request, Vendor will provide You with reasonable information in its possession that may be responsive to the Disclosure Request and any assistance reasonably required for You to respond to the Disclosure Request in a timely manner.

Exhibit 1: Details of Processing of Your Personal Data

This Exhibit 1 includes certain details of the Processing of Your Personal Data as required by Applicable Data Protection Laws.

1. Subject Matter, Nature and Purpose of Processing

The subject matter, nature and purpose of Processing shall be the provision of the Services to You in accordance with the Contract.

2. Duration of Processing

The duration of Processing shall be the term of the Services provided by Vendor to You.

3. Categories of Data Subjects

The types of Data Subject shall be as is contemplated or related to the Processing described in the Contract. This may include, among others, Your employees, contractors, partners, suppliers, and customers.

4. Types of Personal Data

The types of Personal Data shall be as is contemplated or related to the Processing described in the Contract. This may include some or all of the Personal Data identified by engagement type in Vendor's privacy policy and related documentation.

Exhibit 2: Security Measures

Vendor agrees to implement and maintain the following Security Measures:

1. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of Vendor's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Vendor's organization, monitoring and maintaining compliance with Vendor's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include at a minimum logical segregation of data, restricted (e.g., role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Your Personal Data.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.

5. Password controls designed to manage and control password strength, expiration and usage.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of data centers, server room facilities and other areas containing Your Personal Data designed to protect information assets from unauthorized physical access or damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Vendor's possession.

9. Change management procedures and tracking mechanisms designed to test, approve, and monitor all material changes to Vendor's technology and information assets.

10. Incident management procedures designed to allow Vendor to investigate, respond to, mitigate, and notify of events related to Vendor's technology and information assets.

11. Network security controls and procedures for network services and components.

12. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.