DATA PROCESSING ADDENDUM

This **Data Processing Addendum** ("**DPA**") supplements and forms part of the Master Services Agreement (the "**Agreement**") by and between Kairos Performance LLC ("**Kairos**") and the business entity or person identified in the applicable Statement of Work ("**Customer**"). This DPA will become effective on the earlier of the date Customer first uses or accesses the Services or accepts this DPA, or the Agreement or any Statement of Work, which Agreement or Statement of Work incorporates this DPA by reference (the "**DPA Effective Date**")

Capitalized terms used in this DPA have the meanings set forth in this DPA. Capitalized terms used but not otherwise defined herein shall have the meanings given to them in the Agreement. Except as expressly modified below, the terms of the Agreement shall remain in full force and effect.

The parties agree that the terms and conditions set out below shall be added as an addendum to the Agreement. The following obligations shall only apply to the extent required by Data Protection Laws.

1. DEFINITIONS.

1.1. "**Controller**" has the meaning given in Data Protection Laws and, if not defined, means the entity that determines the purposes and means of the Processing of Personal Data and includes a "business" under the CCPA.

1.2. "**Customer Personal Data**" means Personal Data contained in Customer Data that is Processed by Kairos on behalf of Customer to perform the Services under the Agreement.

1.3. "**Data Protection Laws**" means the data privacy and security laws and regulations applicable to the Processing of Customer Personal Data, including, in each case to the extent applicable, European Data Protection Laws, and the California Consumer Privacy Act of 2018 together with its implementing regulations (in each case as amended from time to time, the "**CCPA**").

1.4. "**Data Subject**" means the identified or identifiable natural person who is the subject of Personal Data.

1.5. "**European Data Protection Laws**" means, in each case to the extent applicable: (a) the EU General Data Protection Regulation 2016/679 ("**GDPR**"); (b) the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the Data Protection Act of 2018, and all other laws relating to data protection, the processing of personal data, privacy, or electronic communications in force from time to time in the United Kingdom (collectively, "**UK Data Protection Laws**"); (c) the Swiss Federal Act on Data Protection ("**Swiss FADP**"); and (d) any other applicable law, rule, or regulation related to the protection of Customer Personal Data in the European Economic Area, United Kingdom, or Switzerland that is already in force or that will come into force during the term of this DPA.

1.6. "**Personal Data**" means any information that constitutes "personal information," "personal data," "personally identifiable information," or similar term specifically regulated under applicable Data Protection Laws.

1.7. "**Process**" means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, alignment, combination, restriction, erasure, destruction or disclosure by transmission, dissemination or otherwise making available. "Processed," "Processes," and "Processing" will be interpreted accordingly.

1.8. "**Processor**" has the meaning given in Data Protection Laws and, if not defined, means an entity that Processes Personal Data on behalf of a Controller and includes a "service provider" under the CCPA.

1.9. "**SCCs**" means, as applicable, Module Two (Transfer controller to processor) or Module Three (Transfer processor to processor) of the standard contractual clauses approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (available at http://data.europa.eu/eli/dec_impl/2021/914/oj), as supplemented or modified by **Appendix 3**.

1.10. "**Security Incident**" means a breach of Kairos' security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data in Kairos' possession, custody, or control, which compromises the confidentiality, integrity, or availability of such data. "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

1.11. "**Services**" means the services that Kairos has agreed to provide to Customer under the Agreement.

1.12. "**Subprocessor**" means any Processor appointed by Kairos to Process Customer Personal Data on behalf of Customer under the Agreement.

1.13. "**Supervisory Authority**" means a regulator or other independent competent public authority established or recognized under Data Protection Laws.

2. PROCESSING OF CUSTOMER PERSONAL DATA.

2.1. Roles of the Parties; Compliance. The parties agree that, as between the parties, with regard to the Processing of Customer Personal Data under the Agreement, Customer is a Controller and Kairos is a Processor. In some circumstances, the parties acknowledge that Customer may be acting as a Processor to a third-party Controller in respect of Customer Personal Data, in which case Kairos will remain a Processor with respect to the Customer in such event. Each party will comply with the obligations applicable to it in such role under Data Protection Laws with respect to the Processing of Customer Personal Data.

2.2. Customer Instructions. Kairos will Process Customer Personal Data only in accordance with Customer's documented instructions unless otherwise required by applicable law, in which case Kairos will inform Customer of such Processing unless notification is prohibited by applicable law. Customer hereby instructs Kairos to Process Customer Personal Data: (a) to provide the Services to Customer; (b) to perform its obligations and exercise its rights under the Agreement and this DPA; and (c) as necessary to prevent or address technical problems with the Services. Kairos will inform Customer if it becomes aware that, in its opinion, an instruction of Customer infringes upon Data Protection Laws. Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws. Customer shall be responsible for: (i) giving adequate notice and making all appropriate disclosures to Data Subjects regarding Customer's use and disclosure and Kairos' Processing of Customer Personal Data; and (ii) obtaining all necessary rights, and, where applicable, all appropriate and valid consents to disclose such Customer Personal Data to Kairos to permit the Processing of such Customer Personal Data by Kairos for the purposes of performing Kairos' obligations under the Agreement or as may be required by Data Protection Laws. Customer shall notify Kairos of any changes in, or revocation of, the permission to use, disclose, or otherwise Process Customer Personal Data that would impact Kairos' ability to comply with the Agreement, this DPA, or Data Protection Laws.

2.3. Details of Processing. The parties acknowledge and agree that the nature and purpose of the Processing of Customer Personal Data, the types of Customer Personal Data Processed, the categories of Data Subjects, and other details regarding the Processing of Customer Personal Data are as set forth in **Appendix 1**.

2.4. Processing Subject to the CCPA. As used in this Section 2.4, the terms "Sell," "Share," and "Business Purpose" shall have the meanings given in the CCPA and "Personal Information" shall mean any personal information (as defined in the CCPA) contained in Customer Personal Data. Kairos will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Agreement and this DPA or as otherwise permitted by the CCPA, or (ii) outside of the direct business relationship between Customer and Kairos unless expressly permitted by the CCPA; or (c) combine or update Personal Information with Personal Data received from another source or collected from Kairos' own interaction with the Data Subject, except as expressly permitted by the CCPA. The parties acknowledge that the Personal Information disclosed by Customer to Kairos is provided to Kairos only for the limited and specified purposes set forth in **Appendix 1**. Kairos will comply with applicable obligations under the CCPA, including by providing the same level of privacy protection to Personal Information required by the CCPA. Customer has the right to take reasonable and appropriate steps to help ensure that Kairos uses the Personal Information transferred in a manner consistent with Customer's obligations under the CCPA by exercising Customer's information and audit rights set forth in Section 8. Kairos will inform Customer if it makes a determination that Kairos can no longer meet its obligations under the CCPA. If unauthorized use of Personal Information by Kairos occurs, Customer will have the right, upon written notice to Kairos, to take reasonable and appropriate steps to stop and remediate such unauthorized use by limiting the Personal Information shared with Kairos or such other steps mutually agreed between the parties in writing.

2.5. De-identified Data. If the Agreement requires Kairos to receive and retain de-identified data from Customer, Kairos will: (a) take any necessary measures to ensure that such de-identified data cannot be associated with a Data Subject; (b) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; (c) comply with other applicable restrictions under Data Protection Laws in respect of such de-identified data; and (d) contractually obligate any recipients of the de-identified data to comply with applicable restrictions required by Data Protection Laws.

2.6. No Restricted Countries or Covered Persons. Kairos confirms that it is not a "covered person" as such term is defined in 28 C.F.R. § 202.21. Kairos will take reasonable steps designed to ensure that no Subprocessor is a covered person and that Customer Personal Data will not be accessed by a covered person.

3. CONFIDENTIALITY.

Kairos shall use commercially reasonable efforts to ensure that Kairos personnel who Process Customer Personal Data are subject to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality with respect to such Customer Personal Data.

4. SECURITY.

4.1. Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Kairos shall implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, in accordance with the security standards in **Appendix 2** (the "**Security Measures**"). Customer acknowledges that the Security Measures may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices, provided that the modifications will not materially reduce the overall level of security.

4.2. Security Incidents. Upon becoming aware of a confirmed Security Incident, Kairos will: (a) notify Customer of the Security Incident within 72 hours; and (b) take reasonable steps to identify the cause of such Security Incident, minimize harm, and prevent a recurrence. Kairos will take reasonable steps to provide Customer with information available to Kairos that is reasonably necessary and proportionate for Customer to comply with its obligations under Data Protection Laws. Kairos' notification of or response to a Security Incident under this Section 4.2 will not be construed as an acknowledgement by Kairos of any fault or liability with respect to the Security Incident.

4.3. Customer Responsibilities. Customer agrees that, without limitation of Kairos' obligations under this Section 4, Customer is solely responsible for its use of the Services, including: (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; and (b) securing any account authentication credentials, systems, and devices Customer uses to access or connect to the Services, where applicable. Without limiting Kairos' obligations hereunder, Customer is responsible for reviewing the information made available by Kairos relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

5. SUBPROCESSING.

Subject to the requirements of this Section 5, Customer generally authorizes Kairos to engage Subprocessors as Kairos considers reasonably appropriate for the Processing of Customer Personal Data. A list of Kairos' Subprocessors, including their functions and locations, is available upon Customer's request and may be updated by Kairos from time to time in accordance with this Section 5. Kairos will inform Customer of the addition or replacement of any Subprocessor at least ten (10) days prior to such engagement. Customer may object to such changes on reasonable data protection grounds by providing Kairos written notice of such objection within ten (10) days. Upon receiving such an objection, where practicable and at Kairos' sole discretion Kairos will use commercially reasonable efforts to: (a) work with Customer in good faith to make available a commercially reasonable change in the provision of the Services that avoids using the proposed Subprocessor; or (b) take corrective steps requested by Customer in its objection, subject to mutual agreement and commercial feasibility, and proceed to use the new Subprocessor. Kairos shall be liable for the acts and omissions of the Subprocessor to the extent Kairos would be liable under the Agreement and this DPA.

6. DATA SUBJECT RIGHTS.

If Kairos receives a request from a Data Subject under Data Protection Laws in respect of their Customer Personal Data (such as requests to access, know, correct, delete, restrict, port, object, or opt-out), Kairos will advise the Data Subject to submit the request to Customer. Kairos will, taking into account the nature of the Processing of Customer Personal Data and the functionality of the Services, provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, to assist Customer with fulfilling its obligations under Data Protection Laws to respond to requests by Data Subjects to exercise their rights. Kairos reserves the right to charge Customer on a time and materials basis in the event that Kairos considers that such assistance is onerous, complex, frequent, or time consuming.

7. ASSESSMENTS AND PRIOR CONSULTATIONS.

In the event that Data Protection Laws require Customer to conduct a data protection impact assessment, transfer impact assessment, or prior consultation with a Supervisory Authority in connection with Kairos' Processing of Customer Personal Data, following written request from Customer, Kairos will reasonably assist Customer by providing relevant information and assistance to Customer to fulfil such request, taking into account the nature of Kairos' Processing of Customer Personal Data, the requirements of Data Protection Laws, and the information available to Kairos. Kairos reserves the right to charge Customer on a time and materials basis in the event that such assistance is onerous, complex, frequent, or time consuming.

8. RELEVANT RECORDS AND AUDIT RIGHTS.

8.1. Review of Information and Records. Upon Customer's reasonable written request, Kairos will make available to Customer all information in Kairos' possession reasonably necessary to demonstrate Kairos' compliance with Data Protection Laws and Kairos' obligations set out in this DPA. Such information will be made available to Customer no more than once per calendar year and subject to the confidentiality obligations of the Agreement or a mutually-agreed non-disclosure agreement.

8.2. Audits. If Customer requires information for its compliance with Data Protection Laws in addition to the information provided under Section 8.1, at Customer's sole expense and to the extent Customer is unable to access the additional information on its own, Kairos will allow for, cooperate with, and contribute to reasonable assessments and audits, including inspections, by Customer or an auditor mandated by Customer ("**Mandated Auditor**"), provided that (a) Customer provides Kairos with reasonable advance written notice including the anticipated date of the audit, the proposed scope of the audit, and the identity of any Mandated Auditor, which shall not be a competitor of Kairos; (b) Kairos approves the Mandated Auditor in writing, with such approval not to be unreasonably withheld; (c) the audit is conducted during normal business hours and in a manner that does not have any adverse impact on Kairos' normal business operations; (d) Customer or any Mandated Auditor complies with Kairos' standard safety, confidentiality, and security policies or procedures in conducting any such audits; (e) any records, data, or information accessed by Customer or any Mandated Auditor in the performance of any such audit, or any results of any such audit, will be deemed to be the Confidential Information of Kairos and subject to a nondisclosure agreement to be provided by Kairos; and (f) Customer may initiate such audit not more than once per calendar year unless otherwise required by a documented request from a Supervisory Authority or where legally mandated by Data Protection Laws.

8.3. Results of Audits. Customer will promptly notify Kairos of any non-compliance discovered during the course of an audit and provide Kairos any reports generated in connection with any audit under this Section, unless prohibited by Data Protection Laws or otherwise instructed by a Supervisory Authority. Customer may use the audit reports solely for the purposes of meeting Customer's audit requirements under Data Protection Laws to confirm that Kairos' Processing of Customer Personal Data complies with this DPA.

9. DATA TRANSFERS.

9.1. Data Processing Facilities. Kairos may, subject to Sections 9.2 and 9.3, Process Customer Personal Data in the United States or anywhere Kairos or its Subprocessors maintains facilities or has personnel. Customer is responsible for ensuring that its use of the Services complies with any cross-border data transfer restrictions of Data Protection Laws.

9.2. Transfers of Personal Data Subject to European Data Protection Laws. If Customer transfers Customer Personal Data to Kairos that is subject to European Data Protection Laws, and such transfer is not subject to an alternative adequate transfer mechanism under European Data Protection Laws or otherwise exempt from cross-border transfer restrictions, then Customer (as data exporter) and Kairos (as data importer) agree that the applicable terms of the SCCs shall apply to and govern such transfer and are hereby incorporated herein by reference. In furtherance of the foregoing, the parties agree that: (a) the execution of this DPA shall constitute execution of the applicable SCCs as of the DPA Effective Date; (b) the relevant selections, terms, and modifications set forth in **Appendix 3** shall apply, as applicable; and (c) the SCCs shall automatically terminate once the Customer Personal Data transfer governed thereby becomes lawful under European Data Protection Laws in the absence of such SCCs on any other basis.

9.3. Other Jurisdictions. If Customer transfers Customer Personal Data to Kairos that is subject to Data Protection Laws other than European Data Protection Laws which require the parties to enter into standard contractual clauses to ensure the protection of the transferred Customer Personal Data, and the transfer is not subject to an alternative adequate transfer mechanism under Data Protection Laws or otherwise exempt from cross-border transfer restrictions, then the parties agree that the applicable terms of any standard contractual clauses approved or adopted by the relevant Supervisory Authority pursuant to such Data Protection Laws shall automatically apply to such transfer and, where applicable, shall be completed on a *mutatis mutandis* basis to the completion of the SCCs as described in Section 9.2.

10. DELETION OR RETURN OF CUSTOMER PERSONAL DATA.

Following termination or expiration of the Agreement, Kairos shall, at Customer's option, delete or return Customer Personal Data and all copies to Customer, except as required by applicable law. If Kairos retains Customer Personal Data pursuant to applicable law, Kairos agrees that all such Customer Personal Data will continue to be protected in accordance with this DPA.

11. GENERAL PROVISIONS.

This DPA will, notwithstanding the expiration or termination of the Agreement, remain in effect until, and automatically expire upon, Kairos' deletion or return of all Customer Personal Data. To the extent of any conflict or inconsistency between this DPA and the other terms of the Agreement in relation to the Processing of Customer Personal Data, this DPA will govern. Any liabilities arising in respect of this DPA are subject to the limitations of liability under the Agreement. This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

This Data Processing Addendum was last updated on August 14, 2026.

APPENDIX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

1. Subject matter and duration of the Processing of Customer Personal Data:

The subject matter and duration of the Processing are as described in the Agreement and the DPA.

2. Nature and purposes of the Processing of Customer Personal Data:

The nature of the Processing involves those activities reasonably required to facilitate or support the provision of the Services as described in the Agreement and the DPA.

The purpose of the Processing of Customer Personal Data includes the following:

- Helping to ensure security and integrity, to the extent the use of Customer Personal Data is reasonably necessary and proportionate for these purposes;
- Debugging to identify and repair errors that impair existing intended functionality;
- Short-term, transient use, specifically artificial intelligence operations, revenue operations, and technology consulting services;
- Performing the Services as described in the Agreement and carrying out the instructions set forth in Section 2.2, including providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of Customer;
- Undertaking internal research for technological development and demonstration; and
- Undertaking activities to verify or maintain the quality or safety of the Services, and to improve, upgrade, or enhance the Services.

3. The categories of Data Subjects to whom Customer Personal Data relates:

The categories of Data Subjects are determined by Customer in Customer's sole discretion and may include Customer's employees, business contacts, and customers.

4. The categories of Customer Personal Data:

The categories of Customer Personal Data Processed are those categories permitted by the Agreement and may include business contact information.

5. The sensitive data included in Customer Personal Data:

The parties do not anticipate processing any sensitive data.

6. The frequency of Customer's transfer of Customer Personal Data to Kairos:

On a continuous basis for the term of the Agreement.

7. The period for which Customer Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

As set forth in the DPA or the Agreement.

8. For transfers to Subprocessors, the subject matter, nature and duration of the Processing of Customer Personal Data:

For the same subject matter, nature, and duration set forth above.

APPENDIX 2: SECURITY MEASURES

1. **Information Security Program**. Implement, maintain, and comply with Kairos' written Information Security Policy designed to protect the confidentiality, integrity, and availability of Customer Personal Data and any systems that store or otherwise Process it, which Information Security Policy is: (a) aligned with an industry-standard control framework; (b) approved by executive management; (c) reviewed and updated at least annually; and (d) communicated to all personnel with access to Customer Personal Data.

2. **Risk Assessment**. Maintain risk assessment procedures as appropriate for an organization of Kairos' size, including for the purposes of periodic review and assessment of risks to the organization, monitoring and maintaining compliance with the organization's policies and procedures, and reporting the condition of the organization's information security and compliance to internal senior management.

3. **Personnel Training**. Train personnel to maintain the confidentiality, integrity, and availability of Customer Personal Data, consistent with the terms of the Agreement and Data Protection Laws.

4. **Vendor Management**. Prior to engaging Subprocessors and other subcontractors, conduct reasonable due diligence and monitoring to ensure subcontractors are capable of maintaining the confidentiality, integrity, and availability of Customer Personal Data.

5. **Access Controls**. Only authorized personnel and third parties are permitted to access Customer Personal Data. Maintain logical access controls designed to limit access to Customer Personal Data and relevant information systems (e.g., granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking or changing access when employment terminates or changes in job functions occur).

6. **Secure User Authentication**. Maintain password controls designed to manage and control password strength, expiration, and usage. These include commercially reasonable authentication controls, including multi-factor authentication where available.

7. **Incident Detection and Response**. Maintain a written Incident Response & Data Breach Plan to detect and respond to actual or reasonably suspected Security Incidents and encourage the reporting of such incidents.

8. **Encryption**. Apply industry standard encryption to Customer Personal Data: (a) stored on any medium (i.e., laptops, mobile devices, portable storage devices, file servers and application databases) in high-risk environments or where required by law; and (b) transmitted across any public network (such as the Internet) or wirelessly.

9. **Network Security**. Ensure data is hosted with reputable cloud providers that implement and maintain network security controls and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

10. **Vulnerability Management**. Utilize and maintain industry standard end point protection and software designed to detect, assess, mitigate, remove, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code, and appoint reputable cloud providers for infrastructure vulnerability management.

11. **Change Control**. Adhere to change management procedures as appropriate for an organization of Kairos' size with respect to changes to systems that process Customer Personal Data and as otherwise contemplated by Kairos' written Information Security Policy.

12. **Physical Security**. Take steps to ensure the physical and environmental security of data centers, server room facilities and other areas containing Customer Personal Data, including by: (a) protecting information assets from unauthorized physical access; (b) managing, monitoring, and logging movement of persons into and out of the organization's facilities; and (c) guarding against environmental hazards such as heat, fire, and water damage.

APPENDIX 3: STANDARD CONTRACTUAL CLAUSES

1. **Application of Modules**. If Customer is acting as a Controller with respect to Customer Personal Data, "Module Two: Transfer controller to processor" of the SCCs shall apply. If Customer is acting as a Processor to a third-party Controller with respect to Customer Personal Data, Kairos is a sub-Processor and "Module Three: Transfer processor to processor" of the SCCs shall apply.

2. **Sections I-IV**. The parties agree to the following selections in Sections I-IV of the SCCs: (a) the parties select Option 2 in Clause 9(a) and the specified time period shall be the notification time period set forth in Section 5 of the DPA; (b) the optional language in Clause 11(a) is omitted; (c) the parties select Option 1 in Clause 17 and the governing law of the Republic of Ireland will apply; and (d) in Clause 18(b), the parties select the courts of the Republic of Ireland.

3. **Annexes**. The name, address, contact details, activities relevant to the transfer, and role of the parties set forth in the Agreement and the DPA shall be used to complete Annex I.A. of the SCCs. The information set forth in **Appendix 1** to the DPA shall be used to complete Annex I.B. of the SCCs. The competent Supervisory Authority in Annex I.C. of the SCCs shall be determined pursuant to Clause 13 of the SCCs. The technical and organizational measures in Annex II of the SCCs shall be the measures set forth in **Appendix 2** to the DPA.

4. **Supplemental Business-Related Clauses.** In accordance with Clause 2 of the SCCs, the parties wish to supplement the SCCs with business-related clauses, which shall neither be interpreted nor applied in such a way as to contradict the SCCs (whether directly or indirectly) or to prejudice the fundamental rights and freedoms of Data Subjects. Kairos and Customer therefore agree that the applicable terms of the Agreement and the DPA shall apply to the extent that they are permitted under the SCCs, including without limitation the following: (a) the instructions described in Clause 8.1 are set forth in Section 2.2 of the DPA; (b) in the event a Data Subject requests a copy of the SCCs or the DPA under Clause 8.3, Customer shall make all redactions reasonably necessary to protect business secrets or other confidential information of Kairos; (c) deletion or return of Customer Personal Data by Kairos under the SCCs shall be governed by Section 10 of the DPA; (d) certification of deletion of Customer Personal Data under Clause 8.5 or Clause 16(d) will be provided by Kairos upon the written request of Customer; (e) any information requests or audits provided for in Clause 8.9 shall be fulfilled in accordance with Section 8 of the DPA; (f) the relevant terms of the Agreement which govern indemnification or limitation of liability shall apply to Kairos' liability under Clauses 12(a), 12(d), and 12(f); and (g) the relevant terms of the Agreement which govern termination shall apply to a termination pursuant to Clauses 14(f) or 16.

5. **Transfers from the United Kingdom**. If Customer transfers Customer Personal Data to Kairos that is subject to UK Data Protection Laws, the parties acknowledge and agree that: (a) the template Addendum issued by the Information Commissioner's Office of the United Kingdom and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (available at: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf), as it may be revised from time to time by the Information Commissioner's Office (the "**UK Addendum**") shall be incorporated by reference herein; (b) the UK Addendum shall apply to and modify the SCCs solely to the extent that UK Data Protection Laws apply to Customer's Processing when making the transfer; (c) the information required to be set forth in "Part 1: Tables" of the UK Addendum shall be completed using the information provided in this **Appendix 3** and the DPA; and (d) either party may end the UK Addendum in accordance with section 19 thereof.

6. **Transfers from Switzerland**. If Customer transfers Customer Personal Data to Kairos that is subject to the Swiss FADP, the following modifications shall apply to the SCCs to the extent that the Swiss FADP applies to Customer's Processing when making that transfer: (a) the term "member state" as used in the SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from suing for their rights in their place of habitual residence in accordance with Clause 18(c) of the SCCs; (b) references to the GDPR or other governing law contained in the SCCs shall also be interpreted to include the Swiss FADP; and (c) the parties agree that the Supervisory Authority as indicated in Annex I.C of the SCCs shall be the Swiss Federal Data Protection and Information Commissioner.