DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "**DPA**") forms an integral part of the Master Technology Services Agreement, Master Services Agreement, or any other agreement or contract into which it is incorporated by reference ("**Master Agreement**") between K2 Services LLC and/or its affiliates and subsidiaries (collectively, "**K2**"), and the Client named in the Master Agreement.

For purposes of this DPA, K2 and Client may be referred to individually as a "**party**" and collectively as the "**parties**". This DPA reflects each party's understanding and agreement with regard to the Processing of Client Personal Data. In the event of a conflict between this DPA and the Master Agreement, the terms and conditions set forth in this DPA shall supersede and control with respect to such conflict. For the avoidance of doubt, any provision set forth in the Master Agreement that is neither addressed nor contradicted by this DPA shall remain in full force and effect. Any capitalized term that is used, but not otherwise defined, herein shall be ascribed the meaning set forth in the Master Agreement.

Each party's signature to the Master Agreement shall constitute signature and acceptance of this DPA, including any exhibit or terms attached hereto or otherwise incorporated herein.

1. DEFINITIONS

1.1. **California Consumer Privacy Act** ("**CCPA**") means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 and any other applicable amendments (codified at § Cal. Civ. Code 1798.100 et seq.), and includes any and all implementing regulations thereto.

1.2. **Client Personal Data** means the Personal Data that K2 Processes on behalf of Client.

1.3. **Data Controller** means an entity that determines the purposes and means of the Processing of Personal Data.

1.4. **Data Processor** means an entity that Processes Personal Data on behalf of a Data Controller.

1.5. **Data Protection Law** means all laws, statutes, and regulations applicable to the Processing of Client Personal Data under the Master Agreement, including (when applicable) the CCPA, the GDPR, and the United Kingdom (UK) Data Protection Act 2018.

1.6. **Data Subject** means an identified or identifiable individual whose Personal Data is being Processed by K2.

1.7. **Documented Instructions** means the Processing terms and conditions set forth in the Master Agreement (including this DPA) and any applicable statement of work or similar work order issued thereunder.

1.8. **European Union (EU) Standard Contractual Clauses** means standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.9. **General Data Protection Regulation** ("**GDPR**") means the Regulation 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 and all applicable European Union (EU) Member State legislation implementing the same.

1.10. **Personal Data** means any information or data that, alone or in combination with other information or data, can be used to reasonably identify a particular individual, household, or device, and is subject to, or otherwise afforded protection under, an applicable Data Protection Law.

1.11. **Process, Processing, or Processes** means any action performed on Client Personal Data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, transfer or otherwise making available, alignment or combination, restriction, deletion, or destruction.

1.12. "Security and Privacy Documentation" means the information security and data protection measures that K2 implements and maintains and is available at https://www.K2services.com/securitydocumentation/

1.13. **Security Event** means any unauthorized access, use, loss, acquisition, exfiltration, or disclosure of unencrypted Client Personal Data. A Security Event does not include an Unsuccessful Security Incident.

1.14. **Services** means any professional, advisory, or managed services provided by K2 to Client pursuant to the Master Agreement that involves K2 Processing of Client Personal Data on behalf of Client.

1.15. **Subprocessor** means any third-party organization engaged by K2 to Process Client Personal Data on its behalf.

1.16. **Subprocessor List** means the list of Subprocessors providing Processing services to K2, which may be amended from time to time, and is available at https://www.K2services.com/subprocessors/

1.17. **United Kingdom (UK) Addendum** means the International Data Transfer Addendum to the EU Standard Contractual Clauses (B.1.0) issued by the UK Information Commissioner's Office under S119A(1) Data Protection Act 2018, in force 21 March 2022, and as may be amended or replaced by the UK Information Commissioner's Office or/and Secretary.

1.18. **Unsuccessful Security Incident** means an unsuccessful attempt or activity that does not compromise the security of Client Personal Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

2. SCOPE AND APPLICABILITY; OWNERSHIP

2.1. Scope; Applicability. This DPA applies where and only to the extent that: (i) K2 Processes Client Personal Data on the behalf of Client as a Data Processor in the course of providing Services pursuant to the Master Agreement and (ii) Client is subject to a Data Protection Law. Notwithstanding expiry or termination of the Master Agreement, this DPA will remain in effect until, and will automatically expire upon, deletion or return of all Client Personal Data by K2 to Client.

2.2. Data Ownership. As between Client and K2, Client owns the Client Personal Data and all Client Personal Data shall remain the property of Client. Client hereby grants and agrees to grant to K2 and its affiliates a worldwide, non-exclusive, sublicensable, royalty-free license to Process the Client Personal Data to the extent reasonably necessary to provide, monitor, and modify the Services or as otherwise set forth herein.

2.3. Usage Data. K2 may collect and retain, during and after the term of the Agreement: (i) data that is automatically generated by the Services in connection with Client's use, configuration and deployment of the Services, including patterns identified through the use of algorithms regarding credentialing and access requests, log data and data regarding the performance and availability of the Services and (ii) Client Personal Data that has been anonymized in such a manner that it is not, alone or in combination with other data, reasonably identifiable to Client or any of Client's employees or customers and is aggregated with the data of other clients (such data described in this Section 2.3 (i) and (ii), collectively, "**Usage Data**"). K2 may use and exploit Usage Data for any legal purpose; provided that if K2 provides Usage Data to unaffiliated third parties, such Usage Data shall be presented in a manner that is not, alone or in combination with other data, reasonably identifiable to Client or any of Client's employees or customers.

3. NATURE AND PURPOSE OF PROCESSING; CALIFORNIA DISCLAIMERS

3.1. Roles and Responsibilities. For the purposes of this DPA, the Client shall be considered a Data Controller and K2 shall be considered a Data Processor with respect to Client Personal Data. K2 shall process any Client Personal Data only in accordance with the Documented Instructions, unless required to do otherwise by law. In the event K2 is compelled by law to Process Client Personal Data other than in accordance with the terms and conditions set forth in the Documented Instructions, K2 shall notify Client of that legal requirement prior to Processing, unless such notification is expressly prohibited by law. Additional

Processing by K2 outside the Documented Instructions, if any, will require prior written agreement between K2 and Client.

3.2. Details of Processing. The subject-matter, duration, nature, and purpose of the Processing, the types of Client Personal Data, and the categories of Data Subjects covered by this DPA are set forth in the Master Agreement and this DPA, including Annex I, and, when necessary, supplemented in an additional statement of work or similar work order executed between the parties. The parties agree that Client is solely responsible for determining the types of Client Personal Data uploaded to, and used within, the Services.

3.3. CCPA Disclaimer. For purposes of the CCPA, Client shall be considered a "Business" and K2 shall be considered a "Service Provider." With regard to any Personal Information provided by Client to K2 pursuant to this Master Agreement, K2 hereby acknowledges and agrees that it shall not (i) "Sell" the Personal Information, (ii) retain, use, or disclose the Personal Information for any purpose other than for the specific purpose of performing the Services, or (iii) retain, use, or disclose Personal Information outside of the direct business relationship with Client. Without limiting the foregoing, each party acknowledges and agrees that the provision of Personal Information from Client to K2 does not constitute, and is not the intent of either party for such provision of Personal Information to constitute, a "Sale" of Personal Information, and if valuable consideration, monetary or otherwise, is being provided by Client pursuant to the Master Agreement, such valuable consideration, monetary or otherwise, is so being provided for the Services being rendered and not for the provision of Personal information. For purposes of this Section 3.3 only, the terms "Business," "Service Provider," "Personal Information," "Sale," and "Sell" shall have the same meaning as set forth in the CCPA (Cal. Civ. Code § 1798.140). The limitations set forth in this Section 3.3 shall not be interpreted to prevent K2 from complying with an applicable law, statute, regulation, or a binding order of a governmental or regulatory body.

4. CLIENT OBLIGATIONS

4.1. Accuracy; Compliance. Client shall be responsible for complying with all requirements that apply to it under applicable Data Protection Law and the Documented Instructions it issues to K2. Client acknowledges and agrees that it will be solely responsible for the following: (i) the accuracy, quality, and legality of Client Personal Data, (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Law for the collection and use of the Client Personal Data, including obtaining any necessary consents and authorizations from Data Subjects or otherwise, and (iii) ensuring that the Documented Instructions comply with all applicable laws, statutes, and regulations, including applicable Data Protection Law. For the avoidance of doubt, Client hereby represents to K2 that Client has the legal authority and appropriate business purpose to provide K2 with any and all Client Personal Data in conjunction with the Services, and when legally required, has obtained the consent from all applicable Data Subjects concerning the Processing described herein. Upon request from K2, Client shall provide to K2 within three (3) business days written evidence of such notifications, consents, and authorizations described herein. Client shall inform the Data Processor, immediately and without undue delay (and in any event within 72 hours) if Client is not able to comply with its responsibilities set forth in the Documented Instructions or if the Documented Instructions violate an applicable Data Protection Law, and in either such circumstance, K2 shall be permitted, upon notice to Client, to immediately terminate the Master Agreement or to cease any Processing without being in breach of the Master Agreement.

4.2. Sufficiency. Client is solely responsible for reviewing the Services, including any available security documentation and features (including the Security Documentation), to determine whether they satisfy Client's requirements, business needs, and legal obligations. For the avoidance of doubt, Client is responsible for its use of the Services, including making appropriate use of the Services to ensure a level of security appropriate to the risk with respect to the Client Personal Data, securing its account authentication credentials, protecting the security of Client Personal Data when in transit to and from the Services, taking appropriate steps to securely encrypt and/or backup any Client Personal Data uploaded to the Services, and properly configuring the Services and using available features and functionalities to maintain appropriate security in light of the nature of the Client Personal Data. K2 has no obligation to protect Client Personal Data that Client elects to transmit, store or transfer outside of the Services (e.g., offline or on-premise storage).

5. CONFIDENTIALITY; SECURITY

5.1. Confidentiality. K2 shall maintain the confidentiality of all Client Personal Data and ensure that individuals who are authorized to Process Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.2. Information Security. K2 shall implement and maintain commercially reasonable technical and organizational security controls to protect and safeguard Client Personal Data, which shall include written policies describing its security controls and measures and the relevant procedures and responsibilities of K2 personnel who have access to Client Personal Data ("**Information Security Program**"). K2 shall designate a senior employee to be responsible for the overall management of K2's Information Security Program. The Information Security Program shall include the security controls set forth in Security and Privacy Documentation.

5.3. Updates. K2 may update, amend, or otherwise alter its Information Security Program at any time and without notice to Client, provided that any such update, amendment, or alteration does not increase the likelihood of a Security Event or cause the Information Security Program to not meet the minimum standards set forth herein.

6. DATA SUBJECT AND GOVERNMENT REQUESTS; COOPERATION

6.1. Requests. K2 shall, to the extent legally permitted, promptly notify Client if K2 receives a request from (i) a government or regulatory authority regarding the Processing of, or seeking access to, Client Personal Data ("**Government Data Request**") or (ii) a Data Subject seeking to exercise a data protection right or privilege, such as the right to access or deletion (a "**Data Subject Request**"), and K2 shall, to the extent practicable, seek to direct the requestor to Client. Taking into account the nature of the Processing, K2 shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Government Data Request or a Data Subject Request. In addition, to the extent Client, in its use of the Services, does not have the ability to address the Government Data Request or the Data Subject Request, K2 shall, upon Client's request, furnish commercially reasonable efforts to assist Client in responding to such requests, to the extent K2 is legally required to do so. Client shall be responsible for any costs arising from K2's provision of such assistance described herein. For the avoidance of doubt, Client shall be fully responsible and liable for timely and appropriately responding to a Government Data Request or a Data Subject Request.

6.2. Impact Assessments; Consultation. Upon Client's request, K2 shall (at Client's sole cost and expense) provide Client with commercially reasonable cooperation and assistance (i) needed to fulfil Client's obligation under applicable Data Protection Law to undertake a data protection impact assessment related to Client's use of the Services, to the extent Client does not otherwise have access to the relevant information, and to the extent such information is available to K2 and (ii) with respect to a consultation with a government or regulatory authority.

6.3. Recordkeeping and Disclosures. Client acknowledges that K2 may be required under applicable Data Protection Law to: (i) collect and maintain records of certain information, including the name and contact details of each Data Controller on behalf of which K2 is acting and, where applicable, of such Data Controller's local representative and data protection officer and (ii) make such information available to a government or regulatory authority. Accordingly, to the extent such Data Protection Law applies to the Processing of Client Personal Data, Client will, where requested, provide such information to K2, and will ensure that all information provided is kept accurate and up-to-date.

7. RETURN OR DESTRUCTION OF DATA

7.1. Process and Obligations. On termination or expiration of the Master Agreement, Client may wish to instruct K2 to delete or return all Client Personal Data (including copies) from K2's systems in accordance with applicable Data Protection Law. K2 will, after a recovery period of up to thirty (30) days following expiry or termination of the Master Agreement, comply with this instruction as soon as reasonably practicable, where technically feasible. Client shall be responsible for retrieving any remaining Client Personal Data it wishes to retain before the end of the recovery period. K2 shall not be required to delete or return Client Personal Data to the extent that K2 is required by applicable law or order of a governmental or regulatory body to retain some or all of the Client Personal Data or such Client Personal Data is required for K2 to enforce or defend its legal rights or interests. In addition, except to the extent

required by applicable law, K2 shall not be required to delete or return Client Personal Data archived on back-up systems if K2 shall securely isolate it and protect it from any further Processing and such Client Personal Data is deleted in accordance with K2's standard overwriting and deletion policies.

8. SECURITY EVENT PROCEDURES

8.1. Response Plans. K2 shall establish, implement, and maintain a written incident response plan ("**IRP**") to identify, remediate, respond to, and recover from an actual or a reasonably suspected Security Event. K2 shall undertake IRP-related exercises no less than annually.

8.2. Reporting to Client. Upon confirming a Security Event, K2 shall: (i) taking into account the nature of Processing of Client Personal Data and the information available to K2, notify Client of a Security Event within seventy-two (72) hours from when it discovers the same, (ii) provide timely information to Client relating to the Security Event as it becomes known or as is reasonably requested by Client, and (iii) promptly take reasonable steps to contain, investigate, and mitigate any Security Event and K2 may (in K2's sole and reasonable judgment) retain an independent data incident response consultant to contain, investigate, and remediate the Security Event on its behalf. Client shall fully cooperate with the aforementioned containment, investigation, and remediation of the Security Event and shall not interfere with or otherwise seek to preempt such activities by K2 or its data incident response consultant.

8.3. Incident Notification. K2 will cooperate with Client as reasonably requested by Client in responding to Client's regulators or customers with respect to a Security Event. Notwithstanding the foregoing, Client acknowledges and agrees (i) that K2 will not assess the contents of Client Personal Data in order to identify information subject to any specific legal requirements, (ii) Client shall be solely responsible for notifying or disclosing a Security Event to any applicable government agency, individual, or entity, (iii) Client may not name K2 in consumer or regulatory notifications or press releases without K2's consent (except as required by law), and, (iv) Client shall coordinate with K2 on developing the content of any public statements or any required notices for the affected Data Subjects and/or notices to the relevant supervisory authorities related to the Security Event. Nothing in this DPA shall be interpreted to prevent K2 from complying with its own data incident notification requirements, provided K2 may not name Client in regulatory notifications or press releases without Client's consent (except as required by law), and K2 shall coordinate with Client on developing the content of any public statements or any required regulatory notices related to the Security Event.

8.4. Disclaimers. Any notification, assistance, or cooperation provided by K2 in accordance with this Section 8 shall not be interpreted or construed as an admission of liability, wrongdoing, or fault by K2. To the extent K2 is responsible for the Security Event, subject to the limitations of liability set forth in the Main Agreement, K2 shall be liable for the costs to investigate and respond to the Security Event in accordance with the terms of the Master Agreement.

9. SECURITY REPORTS; AUDITS AND INSPECTIONS

9.1. Security Reports. Upon request, K2 shall provide to Client (on a confidential basis) a summary copy of any third-party audit report or certification applicable to the Services ("**Report**"), so that Client can verify K2's compliance with this DPA. If Client reasonably believes that the Report provided is insufficient to demonstrate compliance with this DPA, K2 shall also provide written responses (on a confidential basis) to reasonable requests for information made by Client related to its Processing of Client Personal Data, including responses to information security and audit questionnaires that are necessary to confirm K2's compliance with this DPA. Client shall not exercise the rights set forth in this Section 9.1 more than once per year.

9.2. Audits; Inspections. If Client reasonably believes that the information provided by K2 pursuant to Section 9.1 is insufficient to demonstrate compliance with this DPA, K2 will allow an audit (including an inspection) by Client, or a third-party auditor appointed by Client and reasonably acceptable to K2, in relation to K2's Processing of Client Personal Data. Any such audit will be at Client's expense, with reasonable advance notice, conducted during normal business hours no more than once per year and subject to K2's reasonable security and confidentiality requirements and provided that the exercise of rights under this Section 9.2 would not infringe Data Protection Laws.

10. SUBPROCESSORS

10.1. Authorized Subprocessors. Client agrees that K2 may, in accordance with this Section 10 of the DPA, engage Subprocessors to Process Client Personal Data on Client's behalf and hereby approves the Subprocessors currently engaged by K2 as set forth in its Subprocessor List.

10.2. Subprocessor Obligations. K2 shall (i) ensure that each Subprocessor is subject to binding obligations that require the Subprocessor to protect the Client Personal Data to the same standard as K2 and (ii) remain responsible for each Subprocessor's compliance with the obligations of this DPA and for any failure by the Subprocessor to fulfil its data protection obligations.

10.3. Changes to Sub-processors. K2 shall inform Client of any intended changes concerning the addition or replacement of a Subprocessor, thereby giving Client the opportunity to object to such changes, provided Client may only object to such changes involving Subprocessors if there are reasonable grounds to believe that the Subprocessor will be unable to comply with the Documented Instructions. If Client objects to K2's use of a new Subprocessor, Client shall notify K2 in writing within ten (10) business days after receiving notification regarding the proposed use of the Subprocessor. Client's failure to object in writing within such time period shall constitute approval to use the new Subprocessor. Client acknowledges and accepts that the refusal to permit the use of a particular new Subprocessor may result in K2's inability to satisfy, in full or in part, the terms and conditions of the Master Agreement, and in such circumstances, Client may terminate the Master Agreement in accordance with the termination provisions of the Master Agreement, and such termination shall not constitute termination for breach of the Master Agreement. K2 may inform Client of any intended changes concerning the addition or replacement of a Subprocessor via email communication, by updating its Subprocessor List, or any other reasonable method that furnishes Client with appropriate notice and opportunity to respond.

11. INTERNATIONAL DATA TRANSFERS

11.1. **EU Standard Contractual Clauses**. Client hereby acknowledges and agrees that, for providing the Services under the Master Agreement, K2 will transfer and retain Client Personal Data in the United States of America. To the extent Client Personal Data originates in the European Economic Area (EEA), the parties undertake to apply the provisions of the EU Standard Contractual Clauses to the transfer and Processing of such Client Personal Data. If the EU Standard Contractual Clauses are applicable between the parties pursuant to this Section 11.1 of this DPA, their provisions will be deemed incorporated by reference into this DPA. To the extent required by the applicable Data Protection Law, the parties shall enter into and execute the EU Standard Contractual Clauses as a separate document. If the parties apply and incorporate the EU Standard Contractual Clauses pursuant to this Section 11.1 of this DPA, then the following shall apply:

11.1.1 Module Two. The EU Standard Contractual Clauses shall be governed by the Module Two (Transfer controller to processor) clauses in all applicable instances, and the Client and/or the Client's EU affiliates shall be the data exporter and K2 shall be the data importer.

11.1.2 Docking Clause. Each party acknowledges and agrees that Clause 7 (Optional – Docking Clause) of the EU Standard Contractual Clauses shall be deemed incorporated therein and applicable to the parties and third parties.

11.1.3 Subprocessing Clause. For purposes of Clause 9(a) (Use of sub-processors) of the EU Standard Contractual Clauses, the parties agree that Option 2 (General Authorization) shall apply to the parties and shall be enforced in accordance with Section 10 and Exhibit C of this DPA.

11.1.4 Redress Clause. For purposes of Clause 11 (Redress) of the EU Standard Contractual Clauses, the parties agree that the optional wording shall not be incorporated therein and therefore shall not be applicable to the parties.

11.1.5 Governing Law. For purposes of Clause 17 (Governing law) of the EU Standard Contractual Clauses, the parties agree that the EU Standard Contractual Clauses shall be governed by the law of Ireland and select Clause 17, "Option 1" to this effect.

11.1.6 Choice of Forum Clauses. For purposes of Clause 18 (Choice of forum and jurisdiction) of the EU Standard Contractual Clauses, the parties agree that any dispute arising from the EU Standard Contractual Clauses shall be resolved by the Courts of Ireland.

11.1.7 Transfer Details (Annex I). Annex I of this DPA shall be incorporated into Annex I of the EU Standard Contractual Clauses.

11.1.8 Security Controls (Annex II). Annex II of this DPA shall be incorporated into Annex II of the EU Standard Contractual Clauses.

11.1.9 Subprocessing List (Annex III). Annex III of this DPA shall be incorporated with the information set forth in the Subprocessor List.

11.1.10 Onward Transfers. K2 shall not transfer Client Personal Data received under the EU Standard Contractual Clauses (nor permit such Client Personal Data to be transferred) to a Subprocessor outside the EEA, unless (i) the Subprocessor is established in a country which the European Commission has granted an adequacy status, or (ii) K2 implements and maintains such measures as necessary to ensure the transfer is in compliance with Data Protection Law, and such measures may include (without limitation) the Subprocessor and K2 executing the EU Standard Contractual Clauses, Module 3 (Transfer processor to processor).

11.2. **UK Addendum**. To the extent Client Personal Data originates in the UK, the parties undertake to apply the provisions of the EU Standard Contractual Clauses, as updated and amended by the UK Addendum, to the transfer and Processing of such Client Personal Data and hereby incorporate the UK Addendum by reference into this DPA, provided the UK Addendum shall be supplemented and completed, as appropriate, with the descriptions and party responsibilities, clause options, and similar criteria set forth in Section 11.1 of this DPA and the Annexes attached hereto. For the avoidance of doubt, with respect to UK data transfers, in the event of a conflict between the EU Standard Contractual Clauses and the UK Addendum, the terms and hierarchy set forth in the UK Addendum shall supersede and control with respect to such UK data transfers only. K2 shall not transfer any Client Personal Data received under the UK Addendum (nor permit such Client Personal Data to be transferred) to a Subprocessor outside the UK, unless the Subprocessor (i) is established in a country which the UK authorities have granted an adequacy status, or (ii) K2 implements and maintains such measures as necessary to ensure the transfer is in compliance with Data Protection Law, and such measures may include (without limitation) the Subprocessor and K2 executing the EU Standard Contractual Clauses, Module 3 (Transfer processor to processor) and the UK Addendum thereto.

11.3. **Data Transfers: Switzerland**. To the extent Client Personal Data originates in Switzerland and K2 is not established in a country which Switzerland or, as applicable, the European Commission, has granted an adequacy status, and K2 has not obtained Binding Corporate Rules authorization in accordance with Data Protection Law, the parties undertake to apply the provisions of the EU Standard Contractual Clauses, as set forth in Section 11.1 of this DPA (and as amended by this Section 11.3), to the transfer and Processing of such Client Personal Data. If the EU Standard Contractual Clauses are applicable between the parties pursuant to this Section 11.3, their provisions will be deemed incorporated by reference into this DPA, and shall apply subject to the following: (i) references to the GDPR in the EU Standard Contractual Clauses are to be understood as references to the Swiss Federal Act on Data Protection (FADP) insofar as the data transfers are subject exclusively to the Swiss FADP and not the GDPR, (ii) the term “member state” in the EU Standard Contractual Clauses shall not be interpreted in such a manner as to exclude Data Subjects in Switzerland from enforcing their rights in Switzerland in accordance with Clause 18(c) of the EU Standard Contractual Clauses, provided Switzerland is their habitual residence, and (iii) for purposes of Annex I(C) of the EU Standard Contractual Clauses, (a) where the data transfer is subject exclusively to the Swiss FADP (and not the GDPR), then the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and (b) where the transfer is subject to both the Swiss FADP and the GDPR, then the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the Swiss FADP, and the supervisory authority set forth in Annex I of this DPA insofar as the transfer is governed by the GDPR.

11.4. **Other Transfers**. To the extent Client Personal Data originates outside of the EEA, Switzerland, or the UK, and the parties seek to transfer and Process such Client Personal Data across national borders, the parties shall also undertake to apply, as appropriate, the provisions of the EU Standard Contractual Clauses or UK Addendum to such transfer and Processing, provided that the EU Standard Contractual Clauses or UK Addendum are legally required and sufficient to meet the requirements of the applicable Data Protection Law for the transfer and Processing of Personal Data across national borders.

11.5 **Surveillance Disclaimers**. If the parties apply and incorporate the EU Standard Contractual Clauses pursuant to Section 11.1 of this DPA or the UK Addendum pursuant to Section 11.2 of this DPA, then K2 hereby represents and warrants the following to be true, accurate, and complete: (i) for the purposes of 50 United States Code (U.S.C.) § 1881(4), K2 is classified as a "electronic communication service provider" and is directly subject to 50 U.S.C. § 1881a ("**FISA § 702**") or provision with a similar effect in your country of residence, (ii) K2 has never been the subject of a FISA § 702 warrant with regard to a request for disclosure of any Personal Data that it Processes, (iii) K2 has never cooperated with public authorities conducting surveillance of communications pursuant to Executive Order (EO) 12333 with regard to Personal Data in K2's custody or control, and (iv) K2 has established internal procedures and processes for responding to FISA § 702 warrants, for cooperating with national security agencies under EO 12333, and for complying with any provision similar to either of the foregoing in the jurisdictions where K2 is located.

11.6. **Changes to the Law**. If and to the extent this DPA or the EU Standard Contractual Clauses or the UK Addendum are no longer recognized by the European Commission or other local privacy authorities as an adequate mechanism for the transfer of Client Personal Data from the European Economic Area, Switzerland, United Kingdom or other country, as applicable, to the United States, then the parties shall abide by another adequate transfer mechanism, provided however that if, after commercially reasonable efforts, K2 is unable to comply with another adequate transfer mechanism, Client or K2 may, upon prior advance written notice to the other party, terminate the Master Agreement and obtain a refund from K2 of pre-paid fees prorated for the remainder of the unused Services as Client's exclusive remedy.

12. MISCELLANEOUS

12.1. Governing Clauses. The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Master Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity, and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Master Agreement.

12.2. Severance. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

12.3. Limitation of Liability. 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 Client affiliates and K2 and K2 affiliates, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Master Agreement and the applicable cap (maximum) for the relevant party set forth in the Master Agreement. 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 Master Agreement and all DPAs together. For the avoidance of doubt, K2 and its affiliates' total liability for all claims from Client and all of Client's affiliates arising out of or related to the Master Agreement and all DPAs shall apply in the aggregate for all claims under both the Master Agreement and all DPAs established under the Master Agreement, including by Client and all Client affiliates, and, in particular, shall not be understood to apply individually and severally to Client and/or to any Client affiliate that is a contractual party to any such DPA. To the extent required by law, (i) this section is not intended to modify or limit either party's liability for Data Subject claims made against a party where there is joint and several liability, or (ii) limit either party's responsibility to pay penalties imposed on such party by a regulatory authority.

12.4. Business Contact Data. Client acknowledges and agrees that it must, from time to time, furnish to K2

certain Business Contact Data pertaining to its employees and other personnel to facilitate the use of the Services or undertake other transactions. Client further acknowledges and agrees that (i) K2 will be considered a data "controller" with respect to such Business Contact Data and K2 will collect, use, and maintain such Business Contact Data in accordance with the K2 Privacy Policy, (ii) Client has the lawful authority to collect and furnish K2 such Business Contact Data, (iii) any Business Contact Data furnished to K2 from Client is accurate and reliable, (iv) Client will promptly notify K2 of staffing or other changes that affect K2' use of the Business Contact Information, and (v) Client has, when required by law, provided notice of all the foregoing to, and received the applicable consent from, any employee or personnel whose Business Contact Data is so provided to K2 under the Agreement. For purposes of this paragraph, the term "**Business Contact Data**" means any personally identifiable information that is used for the purpose of communicating, or facilitating communication, with an individual in relation to their employment, business, or profession, such as the individual's name, position title, and employment-related address, telephone number, or e-mail address

.

Annex I (Data Processing Activities)

A. List of parties:

Name (Data Exporter)	Client
Address	Set forth in the Master Agreement.
Contact person	Set forth in the Master Agreement.
Activities relevant to the data transferred under these Clauses	Set forth below (Section B. Description of Transfer).
Signature and date	By executing the Master Agreement of which this DPA forms an integral part.
Role (controller / processor)	Data Controller.

Name (Data Importer)	K2 Services LLC
Address	Set forth in the Master Agreement.
Contact person	Data Protection Officer, K2DPO@K2services.com
Activities relevant to the data transferred under these Clauses	Set forth below (Section B. Description of Transfer).
Signature and date	By executing the Master Agreement of which this DPA forms an integral part.
Role (controller / processor)	Processor

B. Description of Transfer: Unless otherwise set forth in a statement of work, order form, or similar documentation, the description of the Client Personal Data transferred is as follows:

(i) Categories of Data Subjects: Client may submit Client Personal Data to the Services, the extent of which is determined and controlled by the Client in Client's sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: (i) customers, business partners, and vendors of the Client (who are natural persons), (ii) employees or contact persons of Client's customers, business partners, and vendors, (iii) employees, agents, advisors, contractors, or any user authorized by the Client to use the Service (who are natural persons), and (iv) third parties involved in legal proceedings, litigation, and similar legal matters.

(ii) Categories of Personal Data: Client may submit Client Personal Data to the Services, the extent of which is determined and controlled by the Client in Client's sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Personal Data: names; contact information (addresses, email addresses, telephone numbers); social security numbers, driver's license numbers, passport numbers, and other government identifiers; educational data; IP addresses and other online identifiers; financial data; employment activities; and, location data.

(iii) Sensitive Data: Client may submit Sensitive Data to the Services, the extent of which is determined and controlled by the Client in Client's sole discretion, and which may include, but is not limited to the following categories of Personal Data: health, injury, wellness data; biometric data; race and nationality, immigration status; religion; trade union membership, sex life and sexual orientation; and, information related to an individual's involvement in third parties involved in legal proceedings, litigation, and similar legal matters;

(iv) Transfer Frequency: Continuous and so for so long as Client uses the Services, and for the

termination and transition period thereafter, as set forth in the Master Agreement.

(v) Nature of Processing: For K2 to provide managed services to Client, and to facilitate access and use of the same.

(vi) Purpose of Data Processing: To provide Client access to, and use of, the Services.

(vii) The Period for which Personal Data will be Retained: For the duration of the Master Agreement and for the termination and transition period thereafter, as set forth in the Agreement.

(viii) Subprocessor transfers: The relevant information as set forth in Section 10 and Exhibit III of this DPA.

C. Competent Supervisory Authority: The competent supervisory authority in accordance with Clause 13 of the EU Standard Contractual Clauses is the supervisory authority of Ireland.

Annex II (Security Controls)

K2 shall implement, maintain, and comply with its Security and Privacy Documentation.