Data Privacy Addendum

This Data Privacy Addendum ("Addendum") between Cox and Vendor is made part of the Agreement(s) that incorporate it by reference. The parties wish to supplement the Agreement with the following additional terms. In the event of a conflict between this Addendum and the Agreement, the terms of this Addendum shall prevail.

1. Definitions. Unless otherwise defined herein, all capitalized terms are as defined in the Agreement or the Privacy Laws.

"Affiliate" of Cox means any entity that directly or indirectly (through one or more intermediaries) controls, is controlled by, or is under common control with Cox, where "control" means either the power to direct the management or affairs of the entity or ownership of 50% or more of the voting securities of the entity. Without limiting the generality of the foregoing, affiliates of Cox shall include all entities in which Cox Enterprises, Inc. holds a fifty percent (50%) or greater direct or indirect (e.g., through one or more subsidiaries or Affiliates) interest.

"Personal Information" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to any natural person (including Cox employees), household, or device, and that is collected, received, processed, or otherwise used by Vendor in providing the Services to Company under the Agreement (the "Services"). The term Personal Information includes "Personal Data" and similar terms as defined under the Privacy Laws.

"Privacy Laws" means collectively all applicable privacy, data protection, information security, or related laws or regulations, as revised or amended from time to time.

"Sensitive Personal Information" means (1) government identification information; (2) complete financial account numbers and other financial and credit information (including cardholder data, as defined under the PCI DSS standard); (3) account passwords; (4) genetic, biometric, or health data; (5) racial or ethnic information; (6) political or religious affiliation; (7) trade union membership; (8) information about sex life or sexual orientation; (9) criminal records; (10) the Personal Information of known children under the age of 18; (11) precise geolocation; or (12) other information identified as sensitive or a special category of Personal Information under applicable Data Protection Laws.

2. Status of the Parties. Cox may disclose Personal Information set forth in the then-current Description of Data Processing attached to the Agreement and/or Order Form ("Description of Data Processing") to Vendor for the purpose of Vendor performing Services on behalf of Cox as described in the Agreement. The Parties agree that Cox is the Business/Controller under the Privacy Laws with respect to Cox Personal Information. Vendor is a Service Provider/Processor to Cox under the Privacy Laws.

3. Purpose of Processing. The nature and purpose of Vendor's processing of Personal Information is to perform the Services for Cox as specified in the Agreement and as further described in the Description of Data Processing. The processing of the Personal Information shall continue for the duration of the Agreement, unless otherwise instructed by Cox.

4. Compliance with Applicable Laws. Vendor shall comply with the Privacy Laws. Vendor shall make available to Cox any information Cox may require for purposes of demonstrating its own or Cox's compliance with obligations under applicable Privacy Law, including but not limited to assisting any individual exercise their rights under applicable Privacy Laws and any risk assessments required by law or in accordance with Cox standard policies. Vendor certifies that it understands and will comply with the restrictions set forth herein and under the Privacy Laws. Vendor shall promptly notify Cox if it determines that it can no longer meet its obligations under this Addendum or the Privacy Laws. Cox shall have the right to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information by Vendor.

5. Restrictions on Use of Personal Information. Vendor shall not: (i) retain, use or disclose Personal Information for any purpose other than for the limited and specific business purpose(s) set forth in Section 3 and in accordance with instructions from Cox; (ii) retain, use, or disclose Personal Information for a commercial purpose other than providing the Services to Cox; (iii) "sell" or "share" Personal Information, as defined under the Privacy Laws; (iv) retain, use or disclose Personal Information outside of the direct business relationship between Cox and Vendor; or (v) combine Personal Information received from or on behalf of Cox with Personal Information received from or on behalf of any other person or collected from Vendor's own interaction with a consumer, except as specifically directed by Cox and allowed under the Privacy Laws. Vendor grants to Cox the right, upon notice, to monitor and take reasonable and appropriate steps to ensure that Vendor's use of Personal Information is consistent with each party's respective obligations under the Privacy Laws. Processor will strictly limit access to Cox Personal Information to those Processor personnel performing Services in accordance with the Agreement.

6. Subprocessors. Vendor acknowledges that the restrictions and obligations under the Privacy Laws, this Addendum, and the Agreement apply even if Vendor uses subprocessors in the operation of its business. Vendor may not subcontract or delegate any of its rights or obligations concerning Cox Personal Information without Cox's prior specific written consent, which Cox may withhold in its sole discretion, and only for the purpose of performing the Services specified in the Agreement or as otherwise permitted by the

Privacy Laws. In all such instances, Vendor shall enter into a written agreement with each subprocessor that imposes obligations on such subprocessor that are at least as restrictive as those imposed on Vendor under this Addendum and the Agreement. The subprocessors listed in Exhibit III: Description of Data Processing as "Authorized Subprocessors" as of the effective date are considered approved by Cox unless Cox and/or Vendor learns of additional information regarding such subprocessor that materially impacts the processing of Cox Personal Information as contemplated by the Agreement and this DPA. Vendor shall be liable for the acts and omissions of its subprocessors to the same extent Vendor would be liable if performing the Services of each subcontractor directly under the Agreement.

7. Consumer Requests. Cox will inform Vendor of any consumer request that requires Vendor's compliance and will provide Vendor with the information within Cox's possession that is necessary for Vendor to comply with the request. Vendor will (i) implement and maintain sufficient processes and procedures to satisfy consumer requests; and (ii) Vendor will cooperate with Cox, and promptly (and in any event within fourteen (14) calendar days following notice by Cox, email sufficient) provide any information and documents requested by Cox to respond to requests by consumers under the Privacy Laws. Upon notice of a request for deletion or correction of Personal Information, Vendor will delete or correct (as applicable) the consumer's Personal Information from its systems and records, and notify Vendor's subcontractors to delete or correct the Personal Information (as applicable). If processing a request to delete proves impossible or involves disproportionate effort, Vendor will provide Cox with a detailed explanation of the disproportionate effort required within fourteen (14) calendar days of the date on which Cox notified Vendor of the request to delete. Vendor shall also promptly notify, but no later than two (2) business days, Cox if Vendor directly receives any requests by consumers to exercise their rights under the Privacy Laws related to Vendor's processing of Cox Personal Information. Vendor shall not respond to the request except on the instructions of Cox.

8. Audit; Data Protection Assessments. Upon a minimum of fourteen (14) calendar days' written notice, which may include email, and at least once per annum or indication of non-compliance with applicable Privacy Laws, Vendor shall make available to Cox all information necessary for Vendor to demonstrate compliance with its obligations under this Addendum. Vendor will cooperate with Cox, its internal and external auditors for the purpose of inspecting, examining, and assessing (collectively, "Auditing") Vendor's and any of its subcontractors' compliance with the obligations defined in this Addendum or the Agreement, as it relates to the Services. This Auditing may be conducted through measures including, but not limited to, manual reviews and automated scans, as well as technical and operational testing. Vendor shall promptly provide Cox all information and documents necessary for Cox to conduct and document any data protection assessments as may be required by the Privacy Laws.

9. Confidentiality. Processor will treat all Cox Personal Information as Confidential Information (or as such term is defined in the Agreement), and Processor will not process Cox Personal Information outside the direct relationship with Cox, or for any other purposes, including Processor's own commercial purposes, other than the business purposes specifically outlined in Section 2.3 without Cox's prior written consent. Prior to disclosing Cox Personal Information in response to any public authority request, including requests from regulatory authorities, law enforcement, and courts, Processor will assess the legality of the request and provide notice to Cox to the extent allowed by Processor's legal obligations. In response to any public authority request for disclosure, Processor will only disclose the minimum amount of Cox Personal Information necessary to comply with the valid legal obligation.

10. Security; Incident Response.

10.1 Security. Taking into account the state of the art, implementation costs, the nature of Cox Personal Information, and processing risks, Processor agrees and warrants that it has implemented and will maintain appropriate technical and organizational measures designed to protect Cox Personal Information from unlawful processing and to preserve the security, integrity, availability, confidentiality, and resilience of Cox Personal Information and Processor's processing systems and services. Such measures shall, at a minimum, include the measures described in the DPIS, including any specific measures to protect Sensitive Personal Information and processes for regularly testing, assessing, evaluating, and improving the effectiveness of Processor's security measures.

10.2 Incident Response. Vendor will notify Cox within twenty four (24) hours at privacy@coxinc.com and securityincident@coxinc.com of any actual or suspected unauthorized access to, misappropriation of, loss of, damage to, or other compromise of the security, integrity, availability, or confidentiality of Cox Personal Information (a "Security Incident"). Vendor shall further take all reasonable steps to mitigate any Security Incident at its own cost and shall cooperate with all instructions of Cox in relation thereto. Vendor shall promptly provide any information necessary for Cox's own Security Incident response policies and legal requirements. Vendor shall not make any notification to law enforcement or affected individuals without Cox's prior written consent. Vendor shall make all remediation efforts directed by Cox that Cox determines are reasonable in light of the severity of the Security Incident and be solely responsible for all costs and expenses related thereto, including any third-party costs incurred by Cox in responding to the Security Incident.

10.3 No Conflict. For the avoidance of doubt, this Section 10 is intended to augment the requirements in the DPIS related to Security Incidents. In the event of a conflict, the DPIS shall control.

11. Deletion or Return of Personal Information. Upon receipt of Cox's request or the expiration or termination of the Agreement, Vendor shall, at Cox's election, permanently delete, by securely rendering it unreadable or undecipherable, all Cox Personal Information in Vendor's possession, or, if requested, securely return to Cox, each and every original and copy in every media of all Cox Personal Information in Vendor's or its subcontractor's possession, custody, or control, unless retention of the Personal Information is otherwise specified by Cox or required by law.

12. International Data Transfer. Unless authorized by Cox, Vendor shall not transfer, including permitting access to Personal Information, Cox Personal Information outside of the applicable country in which the Services are to be provided without the prior written approval of Cox. With Cox's prior written approval, Vendor may transfer Cox Personal Information outside of the European Economic Area or the United Kingdom subject to the written instructions set forth in the attached **Exhibit A** (Cross Border Transfers) and such other instructions as Cox may provide to Vendor from time to time.

13. Miscellaneous.

13.1 Allocation of Costs. Unless otherwise stated in this DPA or in the Agreement, each Party will perform its obligations under this DPA at its own costs. Notwithstanding the foregoing, in the event an audit reveals material non-compliance with the terms of this DPA, Vendor shall bear any third party costs related to such audit. In the event of a Security Incident, Vendor shall be liable for all direct damages related thereto, including but not limited to the costs of remediation, attorneys' fees, crisis communications, forensics, notification, and credit monitoring for two (2) years for any impacted individuals.

13.2 Duration of the DPA. This DPA will remain in effect until all Cox Personal Information and copies of it have been returned to Cox or securely deleted.

13.2 Affiliates. References to Cox within this DPA shall be interpreted to include Cox's affiliate(s) to the extent Vendor processes Cox Personal Information on behalf of Cox's affiliates in connection with the Services. For the avoidance of doubt, the foregoing in no way limits any rights of Cox to enforce the Agreement.

13.3 Severability. If any single provision of this DPA is determined to be invalid, unlawful, or unenforceable by a competent court or regulator, the validity and enforceability of the other provisions in this DPA will not be affected. The provision determined to be invalid, unlawful, or unenforceable will continue to be in force in those jurisdictions that do not recognize the competency of the court or regulator making the decision.

EXHIBIT A – CROSS BORDER TRANSFERS
Module 2: Controller-to-Processor

PART 1 – EEA Transfers

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to any transfer of Personal Information outside of the European Economic Area (a "EEA Transfer").
2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Cox as the Controller of the Cox Personal Information and Vendor as the Processor of the Cox Personal Information.
3. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.
4. The General Written Authorization in Clause 9 of the Standard Contractual Clauses shall apply, and the method for appointing and time period for prior notice of Sub-Processor changes shall be as set forth in the DPA.
5. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply.
6. In Clause 13 of the Standard Contractual Clauses, the Supervisory Authority shall be determined by the place of establishment of the data exporter.
7. In Clause 17 of the Standard Contractual Clauses, Option 2 shall apply, and the Parties agree that the Standard Contractual Clauses shall be governed by the laws of Germany.
8. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts located in Germany.
9. Annex I.A of the Standard Contractual Clauses shall be completed as follows:

   Data Exporter: The Cox entities set forth in the Agreement.
   Contact details: As detailed in the Agreement.
   Data Exporter Role: Controller.
   Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

   Data Importer: The Vendor entities set forth in the Agreement.
   Contact details: As detailed in the Agreement.
   Data Importer Role: Processor.
   Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the Agreement.

10. Annex I.B of the Standard Contractual Clauses shall be completed as follows set forth in Appendix 1 of the DPA. In relation to transfers to Subprocessors, the subject matter, nature, and duration of the processing is set forth in the DPA.
11. Annex I.C of the Standard Contractual Clauses shall be completed as follows:

    The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section ~~6~~7 above.
12. The DPIS referred to in the DPA serves as Annex II of the Standard Contractual Clauses.

PART 2 – UK Transfers

1. This Part 2 applies to any transfer of Personal Information subject to the UK GDPR that is transferred outside of the United Kingdom (a "UK Transfer.")
2. With respect to any transfers of Cox Personal Information falling within the scope of the UK GDPR from Cox (as data exporter) to Vendor (as data importer):
   a) neither the Standard Contractual Clauses nor the DPA shall be interpreted in a way that conflicts with rights and obligations provided for in any laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR;
   b) the UK International Data Transfer Addendum (IDTA) version B1.0 in force March 21, 2022 shall apply as follows:
      i) In Table 1 of the UK IDTA (Parties), the parties' details and key contact information shall be as set forth in DPA;
      ii) In Table 2 of the UK IDTA (Selected SCCs, Modules and Selected Clauses), the version of the Approved EU SCCs which this UK IDTA is appended to, including the Appendix Information, shall be as set forth in Part 1 of this Exhibit;
      iii) In Table 3 (Appendix Information) of the UK IDTA:
         (1) Annex 1A: List of Parties: Shall be as set forth in this DPA.
         (2) Annex 1B: Description of Transfer: Shall be as set forth in Appendix 1 of this DPA.
         (3) Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: Shall be as set forth in the DPIS referenced in the DPA.
         (4) Annex III: List of Sub processors: Shall be as set forth in Appendix 1; and
      iv) In Table 4 (Ending this DPA when the Approved Addendum Changes) of the UK IDTA, both the data importer and the data exporter may end the UK IDTA in accordance with the terms of the UK IDTA.

c) Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on February 2, 2022, as it is revised under Section 18 of those Mandatory Clauses.

PART 3 – Additional Safeguards

1. In the event of an EEA Transfer or a UK Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:
   a) Vendor shall have in place and maintain in accordance with good industry practice measures to protect the Cox Personal Information from interception (including in transit from the Cox to the Vendor and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Cox Personal Information whilst in transit and at rest intended to deny attackers the ability to read data.
   b) Vendor will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Cox Personal Information protected under the GDPR or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Court ("FISA").
   c) If Vendor becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Cox Personal Information, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise.
      i) Vendor shall inform the relevant government authority that the Vendor is a processor of the Personal Information and that the Cox Personal Information has not authorized Vendor to disclose the Personal Information to the government authority, and inform the relevant government authority that any and all requests or demands for access to the Personal Information should therefore be notified to or served upon the Cox in writing.
      ii) Vendor will use commercially reasonable legal mechanisms to challenge any such demand for access to Cox Personal Information which is under the Vendor's control. Notwithstanding the above, (a) Vendor acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Cox Personal Information, Vendor has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection shall not apply. In such event, Vendor shall notify Cox, as soon as possible, following the access by the government authority, and provide Cox with relevant details of the same, unless and to the extent legally prohibited to do so.
2. Once in every 12-month period, Vendor will inform Cox at Cox's written request, to the extent permitted by applicable law, of the types of binding legal demands for Cox Personal Information it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.