

## DATA PROTECTION ADDENDUM

This Data Protection Addendum (“**Addendum**”) is attached to and made a part of the Agreement between Supplier and Lumen Technologies Service Group, LLC or one of its affiliates (“**Lumen**”).

### 1. Definitions.

“**Agreement**” means any agreement to which Supplier and Lumen are parties and pursuant to which Supplier Processes any Lumen Personal Data or Lumen Personal Information, whether acting as a licensor or Service Provider to Lumen, authorizing Lumen to resell certain Supplier products, or any other relationship between the parties.

“**Data Subject**” means an identified or identifiable natural person.

“**Privacy Laws**” means all applicable national, federal, state, provincial, or local privacy, cybersecurity, and data protection laws, together with any implementing or supplemental rules, regulations, and regulatory guidance in relation to the Processing and protection of Personal Information or Personal Data including but not limited to: the European Union (“**EU**”) General Data Protection Regulation (Regulation 2016/679) (“**EU GDPR**” or “**GDPR**”); the United Kingdom (“**UK**”) General Data Protection Regulation (“**UK GDPR**”); the Swiss Federal Act on Data Protection (“**FADP**”); the Electronic Communications Data Protection Directive 2002/58/EC; the California Consumer Privacy Act of 2019 (“**CCPA**”) as amended by the California Privacy Rights Act of 2020 (“**CPRA**”); the Colorado Privacy Act (“**CPA**”); the Connecticut Act Concerning Personal Data Privacy and Online Monitoring (“**CTDPA**”); the Delaware Personal Data Privacy Act (“**DPDPA**”); the Florida Digital Bill of Rights (“**FDDBR**”); the Indiana Consumer Data Protection Act (“**ICDPA**”); the Iowa Consumer Data Protection Act (“**ICDPA**”); the Montana Consumer Data Privacy Act (“**MCDPA**”); the New Jersey Data Privacy Act (“**NJDPA**”); the Oregon Consumer Privacy Act (“**OCPA**”); the Tennessee Information Protection Act (“**TIPA**”); the Texas Data Privacy and Security Act (“**TDPSA**”); the Utah Consumer Privacy Act (“**UCPA**”); the Virginia Consumer Data Protection Act (“**CDPA**”); and any regulations promulgated thereto or any other relevant Privacy Laws.

“**Lumen Personal Information**” means Personal Information of Lumen employees, Lumen customers, or any other Personal Information disclosed by Lumen to Supplier or Processed by Supplier on behalf of Lumen.

“**Personal Information**,” which includes “**Personal Data**,” has the meaning set forth in the relevant Privacy Laws.

“**Process**” or “**Processing**” means direct or indirect receipt, access, storage, disclosure, dissemination, transmission, or use of any Personal Data or Personal Information, or the meaning set specifically forth in the relevant Privacy Laws.

“**Restricted Transfer**” means a transfer or an onward transfer of Lumen Personal Information when the transfer would be prohibited by Privacy Laws in the absence of an adequacy decision, a permitted derogation, or protection for the transferred Lumen Personal Information provided by SCCs, or other mechanism specified under applicable Privacy Laws.

“**Standard Contractual Clauses**” or “**SCCs**” means, as applicable to the relevant data transfer, (i) Module 2 (Controller to Processor, applicable when Lumen is the Controller of Lumen Personal Data), or Module 3 (Processor to Processor, applicable when Lumen is Processing Lumen Personal Data on behalf of its Customers) of the standard contractual clauses set out in the 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 (“**EU SCCs**”), (ii) the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018, as amended, (“**UK IDTA**”), or (iii) such other terms intended to provide adequate protection to transferred Lumen Personal Information pursuant to Privacy Laws; in each case, as amended or replaced from time to time under the relevant Privacy Laws.

“**Third Country**” means (i) with respect to GDPR, a country other than the EU Member States; (ii) with respect to the UK Data Protection Law, any country outside of the UK; and (iii) with respect to any other country, as provided in relevant Privacy Laws.

“**UK Data Protection Law**” means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (“**UK GDPR**”), together with the Data Protection Act

2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended), and other data protection or privacy legislation in force from time to time in the United Kingdom.

“**UK IDTA**” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A (1) Data Protection Act 2018, as amended or replaced from time to time by a competent authority under the relevant Privacy Laws.

“**Supplier**” means Supplier or Service Provider and any of its affiliates, agents, representatives, or Sub-Processors, whether or not any such parties are referred to in the relevant clause who may Process Lumen Personal Information. Supplier acknowledges that it may act as a “**Service Provider**” or “**Contractor**” where such term is defined under applicable Privacy Laws.

All other capitalized terms used herein shall have the meaning set forth in the relevant Privacy Laws, or as specified elsewhere in the Agreement(s).

2. **Compliance with Privacy Laws.** Supplier guarantees it will implement appropriate administrative, technical, and physical controls in such a manner that Processing under this Addendum will meet the requirements under applicable Privacy Laws. Supplier shall promptly, and without undue delay, notify Lumen if Supplier determines that it can no longer meet its obligations under applicable Privacy Laws or this Addendum.
3. **Restriction on Sub-Processors.**
  - a. Lumen authorizes Supplier to engage other parties for Processing Lumen Personal Information (each such party, a “Sub-Processor”). Supplier shall maintain a list of all Sub-Processors engaged by Supplier to be provided to Lumen upon request. Supplier shall provide Lumen with prior written notice of any changes to its Sub-Processors, and Lumen shall have thirty (30) days to object to such change.
  - b. Notwithstanding the foregoing, Supplier shall only engage such Sub-Processor for conducting the specific Processing activities authorized by Lumen pursuant to the terms of a written agreement containing the same obligations as set forth herein with respect to such Sub-Processor’s Processing of Lumen Personal Information. In the event any Sub-Processor fails to fulfil its obligations under such written agreement, Supplier shall remain fully liable to Lumen for the performance of such Sub-Processor’s obligations.
4. **Processing.** When Processing Lumen Personal Information, Supplier shall (and shall procure that its affiliates and Sub-processors shall):
  - a. Document the duration, nature, and purpose of the Processing for specific services, along with the type of Lumen Personal Information and categories of Data Subjects separately in Statements of Work, Order Forms, and similar attachments to the Agreement.
  - b. Only Process Lumen Personal Information on Lumen’s documented instructions. If Supplier believes that Lumen’s instructions infringe, or are likely to infringe, applicable law, Supplier shall immediately notify Lumen of the same. Supplier shall not engage in any Processing until the parties have resolved the legality of the Processing. If Supplier is required to Process Lumen Personal Information for a reason other than as instructed by Lumen pursuant to applicable law to which the Supplier is subject, Supplier shall inform Lumen of that legal requirement prior to engaging in any additional Processing, unless applicable law prohibits such disclosure.
  - c. Ensure that persons authorized to Process Lumen Personal Information are subject to appropriate confidentiality requirements.
  - d. At Lumen’s option, permanently destroy or return all Lumen Personal Information after the end of the provision of services relating to Processing of such Lumen Personal Information and permanently destroy all existing copies of such Personal Information in accordance with the terms set forth herein unless applicable law requires Supplier to maintain such Personal Information. In the event Supplier retains such Personal Information pursuant to legal requirements, Supplier shall (i) provide Lumen with written notice of such requirements; (ii) continue to protect such retained Personal Information in accordance with this Addendum; and (iii) only use such retained Personal Information to fulfil Supplier’s obligations under applicable legal requirements. Proper destruction methods include those widely recognized in the industry as sufficiently rendering retrieval, restoration, or reconstruction of any Lumen Personal Information practicably impossible, regardless of the form or media. Upon Lumen’s request, Supplier shall cause an executive officer of Supplier to formally certify, in form and content reasonably satisfactory to Lumen, that Supplier has complied with the foregoing secure destruction requirements.

- e. Notify Lumen in writing or electronically, within five (5) calendar days, if Supplier receives a request to exercise access rights from a Data Subject relating to that individual's Personal Information (a "Data Subject Request"). Supplier shall not otherwise communicate with an individual regarding such Data Subject Request unless Lumen directs Supplier to do so. Supplier shall, in a manner consistent with the nature and functionality of the services provided in the Agreement and Supplier's role as a Processor or Service Provider, provide reasonable assistance to Lumen to enable Lumen to comply with its obligation to respond to a Data Subject Request, including, but not limited to, providing, deleting, or correcting any Lumen Personal Information in Supplier's possession.
- f. Maintain a Record of Processing activities conducted for and on behalf of Lumen in accordance with applicable Privacy Laws. Where applicable, those records shall include information about transfers of Lumen Personal Information to a Third Country or an international organization; the identification of that Third Country or international organization; and, in the case of transfers to a Third Country that does not provide adequate protection for Personal Data within the meaning of Article 45 of the GDPR, documentation of the suitable safeguards implemented to enable such transfer.
- g. Fully cooperate with Lumen to enable Lumen to complete any privacy or data protection impact assessments that Lumen deems necessary (in its sole discretion) under Article 35 of the GDPR or applicable Privacy Laws related to Processing of Lumen Personal Information undertaken by Supplier
- h. Cooperate, where applicable and on request, with any governing body's performance of its tasks mandated under the relevant Privacy Laws.

## **5. United States Processing Requirements.**

- a. In addition to the Processing requirements outlined above, Supplier shall not: (i) sell, or share Lumen Personal Information; (ii) collect, retain, use, or disclose Lumen Personal Information for any purpose, including any commercial purpose, other than providing Services specified in the agreement(s) between Lumen and Supplier; (iii) collect, retain, use, or disclose Lumen Personal Information outside of the direct business relationship between Lumen and Supplier; or (iv) combine Lumen Personal Information with other Personal Information that Supplier obtains from other sources or that Supplier collects itself. Supplier acknowledges that Lumen Personal Information shall only be Processed pursuant to Lumen's instructions or a "**Business Purpose**" including those Business Purposes outlined separately in Statements of Work, Order Forms, and similar attachments to the Agreement. Supplier understands that Lumen may exercise any right of a Controller or Business under Privacy Laws including, but not limited to, any right that: (a) permits Lumen to take reasonable and appropriate steps to ensure that Supplier uses Lumen Personal Information consistent with Lumen's Business Purpose; and/or (b) stops or remediates Supplier's unauthorized use or misuse of Lumen Personal Information, upon notice to Lumen. Without unreasonable delay, but no later than five (5) days, Supplier shall notify Lumen if it can no longer meet its obligations under US Privacy Law. Supplier certifies that it understands the prohibitions outlined in this Section 5(a) and will comply with them.
- b. CCPA. As required specifically by the CCPA, Supplier certifies that it has read and understands and will strictly comply with the applicable requirements of the CCPA. The parties acknowledge that Supplier is a Service Provider and not a Third Party. Any Lumen Personal Information is disclosed or received only for limited and specified business or commercial purposes, and Supplier acknowledges and agrees that Lumen does not sell or share the Personal Information of California residents in connection with the services. Accordingly:
  - i. Supplier shall not: (i) sell, share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Lumen Personal Information to any third party for monetary or other valuable consideration; (ii) collect, retain, use, or disclose Lumen Personal Information outside of the business relationship between the parties, unless otherwise permitted by the CCPA; (iii) further collect, sell, or use Lumen Personal Information except as necessary to perform the specific Business Purpose for which Supplier was retained, (iv) combine Lumen Personal Information with Personal Information received from or on behalf of another party(s), or collected from Supplier's own interactions with individuals, unless permitted by CCPA, and (v) collect, use, retain, or disclose sensitive Lumen Personal Information except as directed by Lumen in writing or otherwise permitted by CCPA.
  - ii. If Supplier collects Personal Information directly from consumers on behalf of Lumen, Supplier shall provide all required CCPA-compliant notices at the time of such collection.
  - iii. If Lumen provides Supplier with deidentified Lumen Personal Information, or if Supplier deidentifies Lumen Personal Information, Supplier agrees to (i) take reasonable measures to ensure that such deidentified Personal Information cannot be associated with a consumer or household, (ii) not attempt to reidentify such Personal

Information, and (iii) contractually obligate any further recipient to comply with all provisions of this Addendum.

## 6. Transfers.

- a. Under the requirements of the GDPR, Supplier shall not transfer any Lumen Personal Data to any Third Country or international organization without Lumen's written consent. Lumen's consent to Supplier's transfer of any Lumen Personal Data to a Third Country or international organization shall be conditioned on the existence of one of the following circumstances:
    - i. The transfer is to a country that is a member of the European Economic Area ("EEA");
    - ii. The transfer is to a country, or a territory or specified sector within such country, or to an international organization that is deemed to provide an adequate level of protection for Lumen Personal Data in accordance with Article 45 of the GDPR;
    - iii. The transfer is subject to appropriate safeguards, including the condition that enforceable Data Subject rights and effective legal remedies for the Data Subject are available in accordance with Article 46 of the GDPR; or
    - iv. The purpose of the transfer falls within one of the specified situations set forth in Article 49 of the GDPR; provided, however, Supplier shall not transfer any Lumen Personal Data under this Section without Lumen's prior written consent.
  - b. Transfer(s) performed pursuant to Section 6(a) above will be subject to the SCCs as outlined below. It is not the intention of either Party to contradict or restrict any of the provisions set forth in SCCs and, accordingly, if and to the extent SCCs conflict with any provision of the Agreement (including this DPA), SCCs shall prevail to the extent of such conflict.
  - c. EU SCCs. Where Supplier transfers Lumen Personal Data from the EEA or otherwise protected by the EU GDPR, the EU SCCs shall apply as follows: (i) Module 2 (Controller to Processor is applicable when Lumen is the Controller of Lumen Personal Data), and Module 3 (Processor to Processor is applicable when Lumen is Processing Lumen Personal Data on behalf of its Customers) (ii) in Clause 7, the optional docking clause will not apply; (iii) in Clause 9, Option 2 will apply and the time period for prior notice of Sub-processor changes will be as set forth in this DPA; (iv) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of the Republic of Ireland; (vi) in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland;
    - i. Annex I, Part A, List of Parties, is completed with the following information:
      - Data exporter(s): Lumen (or its affiliate)
      - Contact details: as provided in the Agreement
      - Data exporter role: Controller or Processor (as applicable)
      - Signature and date: by entering into this DPA, Data Exporter is deemed to have incorporated these EU SCCs and Annexes
    - Data importer(s): Supplier
    - Contact details: as provided in the Agreement
    - Data importer role: Processor
    - Signature and date: by entering into this DPA, Data Importer is deemed to have incorporated these EU SCCs and Annexes
  - ii. Annex I, Part B, Description of Transfer, will be outlined separately in Statements of Work, Order Forms, and similar attachments to the Agreement.
  - iii. Annex I, Part C, Competent Supervisory Authority, is completed with the following information: the Irish Data Protection Commission;
  - iv. Annex II, Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data, is completed with the information specified in Section 7 (Information Security Measures) of this DPA; and
  - v. Annex III, List of Sub-processors, will be provided by Supplier.
- d. Swiss FADP. Where Supplier transfers Lumen Personal Data protected by FADP, the EU SCCs will apply, amended and adapted as follows: (i) in Clause 13, the Swiss Federal Data Protection and Information Commissioner is the

exclusive competent Supervisory Authority; (ii) references to the term “member state” must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18; and (iii) references to “General Data Protection Regulation,” “Regulation 2016/679,” and “GDPR” in the EU SCCs shall also include the reference to the equivalent provisions of the Swiss Federal Act on Data Protection (“FADP”) (as amended or replaced).

- e. UK IDTA. Where Supplier transfers Lumen Personal Data protected by the UK GDPR, the UK IDTA applies as follows: (a) the EU SCCs, completed as set out above, shall also apply to transfers of UK Lumen Personal Data; and (b) the UK IDTA shall be deemed executed between the Parties, and the EU SCCs shall be deemed amended as specified by the UK IDTA in respect of the transfer. The competent Supervisory Authority for UK Personal Information protected by the UK GDPR shall be the Information Commissioner’s Office.
- f. Supplier shall inform Lumen of developments that might lead to Supplier’s inability to comply with its obligations under this DPA (including the SCCs). In the event of any such change, Lumen shall be entitled to immediately (i) suspend the transfer of Lumen Personal Information, (ii) terminate this DPA, and/or (iii) require Supplier to return or delete Lumen Personal Information.
- g. Under GDPR, if Supplier receives legal process requiring disclosure of Lumen Personal Information to a public authority in a Third Country that does not benefit from an EU adequacy decision, Supplier shall promptly, and as applicable: (i) inform the relevant public authority of the incompatibility of the legal process with the safeguards provided under this DPA, and the resulting conflict of obligations for Supplier; (ii) promptly notify Lumen of the legal process and provide a copy, unless legally prohibited from doing so; (iii) assess the lawfulness of the legal process; (iv) respond to the legal process by using reasonable efforts to challenge the validity of the legal process where there are grounds to do so; (v) seek interim measures to suspend the effects of the legal process until the relevant court or authority has decided on the merits; (vi) refrain from disclosing the Lumen Personal Information until required to do so under the applicable procedural rules; and (vii) provide the minimum amount of Lumen Personal Information permissible when responding to the legal process, based on a reasonable interpretation thereof.
- h. Supplier shall maintain a written record of all transfers to Third Countries or international organizations made pursuant to this Section and shall make a copy of such record available to Lumen and/or any Supervisory Authority upon request.

**7. Information Security Measures.** In addition to, and not in lieu of, any information security requirements set forth in the Agreement, Supplier shall implement appropriate administrative, technical, organizational, and physical controls to ensure that Supplier’s Processing of Lumen Personal Information complies with all requirements under applicable Privacy Laws and is protected against accidental or unlawful Processing, destruction, loss, alteration, unauthorized disclosure of, or access. Such controls, to the extent appropriate under the circumstances and taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of the Processing, shall meet or exceed the requirements of the Information Security Requirements found at Lumen’s Supplier Portal ([Information Security Requirements \(lumen.com\)](#)). In addition, Supplier shall:

- a. Pseudonymize and/or encrypt all Lumen Personal Information;
- b. Take reasonable steps to ensure reliability and integrity of any Supplier personnel or permitted Sub-Processor who have access to Lumen Personal Information and appropriate measures to ensure that such parties are informed of the confidential nature of such Personal Information and comply with the obligations set forth in this Addendum;
- c. Conduct regular testing, assessing, and evaluating the effectiveness of the technical and organizational measures of the information systems for ensuring the security of Processing;
- d. Take reasonable steps to ensure the ability to restore the availability and access to Lumen Personal Information in a timely manner in the event of a physical or technical incident; and
- e. Take reasonable steps to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services utilized to Process Lumen Personal Information.

**8. Right to Audit; Requirement to Provide Compliance Records.** Supplier shall allow, and cooperate with, reasonable assessments by Lumen or Lumen’s designated assessor on an annual basis (or more frequently if Supplier experiences a Security Incident). Supplier may instead arrange for a qualified and independent assessor to conduct an assessment of Supplier’s policies and technical and organizational measures in support of the obligations under applicable Privacy Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and Supplier shall provide a report of such assessment to Lumen upon request.

9. **Security Incident.** Supplier shall notify Lumen if Lumen Personal Information was, or is reasonably believed to have been, accessed, and/or acquired by an unauthorized person (a “Security Incident”) without undue delay and in no event later than forty-eight (48) hours. Supplier shall notify Lumen of any facts known to Supplier regarding the Security Incident and cooperate fully with Lumen to mitigate and remediate the Security Incident. Supplier shall be deemed to be aware of a Security Incident when Supplier has a reasonable degree of certainty that a Security Incident has occurred. At a minimum and where available, the notification of a Security Incident shall include the following:
- a. Description of the nature of the Security Incident including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Lumen Personal Information records concerned;
  - b. The name and contact details of Supplier’s Data Protection Officer, if applicable, or other contact point where additional information can be obtained;
  - c. Description of the likely consequences of the Security Incident; and
  - d. Description of the measures taken or proposed to be taken by Supplier to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects.

In the event Supplier does not have all the information referenced above at the time it provides its initial notification to Lumen of a Security Incident, Supplier shall continue to investigate such Security Incident and provide the above-referenced information as it becomes available.

10. **Indemnification.** Supplier shall defend, indemnify, and hold harmless Lumen from and against any and all claims, suits, liabilities, expenses, attorney’s fees, or damages arising because of claims related to Processing or protection of Lumen Personal Information within the Supplier’s control or Supplier’s alleged or actual breach of the terms of this Addendum.
11. **No Limitation of Liability.** Notwithstanding anything to the contrary in any Agreement, any and all limitations of liability or other caps on damages set forth in any Agreement shall not apply to any damages arising out of or relating to Supplier’s breach of the terms of this Addendum.
12. **Interpretation with Agreement.** This Addendum is intended to supplement the Agreement between the parties and not replace existing obligations. This Addendum is subject to the terms and conditions of the Agreement and shall be deemed part of the Agreement. In the event of a conflict between the Agreement and this Addendum, this Addendum shall prevail; provided, however, if such conflict arises as a result of multiple obligations with respect to security, data protection, or privacy, the stricter obligation shall apply. Supplier’s failure to comply with any of the provisions of this Addendum shall be deemed a material breach of the Agreement.