SYNOVIA DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") is effective on the first date that Customer provides to Synovia Customer Personal Data (as defined below) subject to the applicable Privacy Law (as defined below) and forms part of the Principal Agreement or other written or electronic agreement ("**Agreement**") by and between the organization signing or accepting below ("**Customer**") and Synovia Solutions LLC ("**Synovia**"), and sets forth the terms and conditions relating to the privacy, confidentiality, and security of Customer Personal Data associated with Synovia Products and subscription and maintenance services to be rendered by Synovia to Customer pursuant to the Agreement. All terms defined or used in the Agreement shall have the same meaning in this Addendum unless otherwise specified. Terms used in this Addendum which are not defined herein or in the Agreement shall have the meaning set forth in the applicable Privacy Law.

Whereas Customer may provide Synovia, a company located in the United States, with access to Customer Personal Data, Personal Information or Personally Identifiable Information to act as a Processor or Service Provider in connection with Synovia Products and subscription and maintenance services performed by Synovia for or on behalf of Customer pursuant to the Agreement; and

Whereas Customer requires that Synovia preserve and maintain the privacy and security of such Customer Personal Data as a Processor according to the terms of this Addendum;

Now therefore, in consideration of the mutual covenants and agreements in this Addendum and the Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Customer and Synovia agree as follows:

1. **Definitions and Interpretation**.
   - 1.1 "**Contracted Processor**" means a Subprocessor.
   - 1.2 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Customer pursuant to or in connection with the Principal Agreement.
   - 1.3 "**DPA**" means this Data Processing Addendum .
   - 1.4 "**Data Protection Laws**" means EU Data Protection Laws (European Union General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) and The California Consumer Privacy Act of 2018, as amended or other privacy laws applicable to Synovia.
   - 1.5 "**Data Transfer**" means:
     - (a) a transfer of Customer Personal Data from the Customer to a Contracted Processor; or
     - (b) an onward transfer of Customer Personal Data from a Contracted Processor to a Sub processor, or between two establishments of a Contracted Processor in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws).
   - 1.6 "**EEA**" means the European Economic Area.
   - 1.7 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.
   - 1.8 "**GDPR**" means EU General Data Protection Regulation 2016/679.
   - 1.9 "**Services**" means the Devices and Data services Synovia provides.
   - 1.10 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Customer in connection with the DPA.

2. **Processing of Customer Personal Data.**
   - 2.1 With respect to Customer Personal Data, Customer is the Controller and Synovia is the Processor. Where Data Protection Laws use different terminology, Customer is the "business," "controller," or equivalent, and Synovia is the "service provider," "processor," "contracted service provider," or equivalent. Synovia is a Processor for all Processing of Customer Personal Data under this DPA and does not act as an independent Controller with respect to such data.
   - 2.2 Processor shall:
     - (a) comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and
     - (b) not Process Customer Personal Data other than on the relevant Customer's documented instructions.
     - (c) immediately inform Customer if, in its opinion, an instruction infringes Data Protection Laws. Synovia may suspend Processing pursuant to a disputed instruction pending resolution, without liability.
   - 2.3 2.3 Synovia shall not:
     - (a) sell or Share Customer Personal Data, as those terms are defined in the CCPA;
     - (b) retain, use, or disclose Customer Personal Data for any purpose other than the specific Business Purposes specified in the Principal Agreement.

3. **Processor Personnel**. Processor shall take reasonable steps to ensure the reliability of any employee, agent, or contractor of any Contracted Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. **Security.**
   4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
   4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. **Subprocessing**.
   5.1 General authorization. Customer grants Synovia general written authorization to engage Subprocessors.
   5.2 Notice and objection. Synovia shall notify Customer of any intended addition or replacement of a Subprocessor at least thirty (30) days before that Subprocessor Processes Customer Personal Data, by email to Customer's designated contact. Customer may object on reasonable data-protection grounds within fifteen (15) days of notice. If the Parties cannot resolve the objection within thirty (30) days, Customer may terminate the affected Services without penalty and with a pro-rata refund of prepaid fees.
   5.3 Synovia shall impose on each Subprocessor, by written contract, data protection obligations that are no less protective than those in this DPA, including the obligations in Article 28(3) of the GDPR and, where applicable, the CCPA service provider terms in Section 2.3. Where the Subprocessor is located outside the EEA, UK, or Switzerland, Synovia shall ensure a valid transfer mechanism under Section 11 is in place, including by executing the SCCs (Module 3) or IDTA as applicable.

6. **Data Subject Rights**.
   6.1 Taking into account the nature of the Processing, Processor shall assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
   6.2 Processor shall:
      (a) promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and
      (b) ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

7. **Personal Data Breach.**
   7.1 Processor shall notify Customer without undue delay upon Processor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
   7.2 Processor shall co-operate with the Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8. **Data Protection Impact Assessment and Prior Consultation**. Processor shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by Articles 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. **Deletion or return of Customer Personal Data.**
   9.1 Subject to this Section 9, upon the termination or expiration of the Services involving the Processing of Customer Personal Data and at Customer's written request, Synovia shall, within a commercially reasonable period not to exceed thirty (30) days, delete or return Customer Personal Data and delete

existing copies, unless applicable law requires retention of the Customer Personal Data. Notwithstanding the foregoing, Synovia may retain Customer Personal Data contained in archival backup systems, disaster recovery systems, security logs, audit records, or records required to comply with legal, regulatory, tax, accounting, or litigation-hold obligations, provided that such retained Customer Personal Data shall remain subject to the confidentiality, security, and other applicable provisions of this DPA and shall not be further Processed except as required by applicable law or for such permitted retention purposes.

9.2 Upon Customer's written request, Synovia shall provide written confirmation that it has complied with its obligations under this Section 9. To the extent Customer Personal Data is retained pursuant to Section 9.1, Synovia shall identify the categories of retained data and the basis for such retention upon reasonable request .

10. **Audit rights.**

10.1 Subject to this section 10, Processor shall make available to the Customer on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Customer only arise under Section 10.1 to the extent that the DPA does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. **Data Transfer**. Synovia may transfer Customer Personal Data to the United States or other jurisdictions as necessary to provide the Services, provided that such transfer is made in accordance with a valid transfer mechanism under applicable Data Protection Laws, including the mechanisms set forth below .

11.1 **EU-U.S. Data Privacy Framework / UK Extension / Swiss-U.S. DPF.** To the extent Synovia is certified under the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. Data Privacy Framework (collectively, "DPF") as administered by the U.S. Department of Commerce, transfers of Customer Personal Data from the EEA, the United Kingdom, or Switzerland to Synovia in the United States may be made in reliance on Synovia's applicable DPF certification as an adequate transfer mechanism under the relevant adequacy decision or recognition. Synovia shall maintain its DPF certification(s) in active status throughout the term of this DPA and shall promptly notify Customer in writing in the event that any DPF certification is withdrawn, lapses, or is otherwise no longer valid. Upon any such lapse or withdrawal, the Parties shall promptly implement an alternative transfer mechanism in accordance with subsection (b) below.

11.2 **Standard Contractual Clauses.** Where a DPF certification is not available or is no longer in effect with respect to a particular transfer, the Parties shall rely on the EU-approved Standard Contractual Clauses adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("2021 SCCs"), or such successor SCCs as may be approved by the European Commission, together with any applicable supplementary measures required by competent supervisory authority guidance. For transfers from the United Kingdom, the Parties shall execute the International Data Transfer Addendum (IDTA) issued by the UK Information Commissioner's Office (or its successor), as applicable.

11.3 **Alternative Adequacy Mechanisms.** The Parties may rely on any other transfer mechanism recognized as providing an adequate level of protection under applicable Data Protection Laws (including an adequacy decision issued by the European Commission or a competent UK authority), provided that the applicable mechanism is valid and in force at the time of transfer.

The Parties agree that the transfer mechanisms in subsections (a) through (c) shall be applied in the order of preference listed, with the DPF certification serving as the primary mechanism to the extent it covers the relevant transfer, and SCCs serving as the fallback. Nothing in this Section 11 shall require the use of SCCs where a valid DPF certification or other adequacy mechanism applies to and covers the relevant transfer.

12. **General Terms.**

12.1 **Confidentiality**. Each Party must keep this DPA and information it receives about the other Party and its business in connection with this DPA ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law; or

(b) the relevant information is already in the public domain.

12.2 **Notices**. All notices and communications given under this DPA must be in writing and will be delivered personally, sent by post, or sent by email to the address or email address set out in the heading of the Principal Agreement at such other address as notified from time to time by the Parties changing address.

13. Illinois Biometric Information Privacy Act (BIPA).

13.1 **Applicability.** This Section 13 applies to the extent that Synovia's Services involve the collection, capture, storage, use, or transmission of Biometric Data (as defined in Section 13.2) from or relating to individuals physically present in Illinois or who are Illinois residents ("Illinois Biometric Processing"). This Section 13 supplements the other provisions of this DPA and, to the extent of any conflict between this Section 13 and any other provision of this DPA with respect to Biometric Data, this Section 13 shall control. The Parties acknowledge that the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 et seq., as amended ("BIPA"), may impose independent obligations on each Party in connection with Biometric Data and that the allocation of responsibilities in this Section 13 reflects the Parties' reasonable business understanding but does not constitute a legal determination regarding the ultimate allocation of BIPA compliance obligations.

13.2 **Definitions.** For purposes of this Section 13, the following terms shall have the meanings set forth below.

(a) "**Biometric Data**" means any "biometric identifier" or "biometric information" as defined under BIPA, including scans of face geometry, voiceprints, retina or iris scans, and fingerprints, and any information derived therefrom that is used to identify an individual. For the avoidance of doubt, Biometric Data does not include photographs, video footage that has not been processed to extract biometric identifiers, writing samples, written signatures, or demographic data (such as height, weight, hair color, or eye color).

(b) "**Biometric Feature**" means any Synovia product feature or service capability that collects, stores, processes, or transmits Biometric Data, including without limitation driver-facing camera functionality with AI-based facial analysis, and Camera ID or AI-based driver identification features. Synovia shall provide Customer with written notice identifying all then-current Biometric Features upon request and no later than thirty (30) days prior to introducing any new Biometric Feature.

(c) "**BIPA Written Release**" means a written release satisfying the requirements of 740 ILCS 14/15(b), consisting of: (i) written disclosure that Biometric Data is being collected or stored, identifying the specific type of Biometric Data; (ii) disclosure of the specific purpose and length of time for which Biometric Data will be collected, stored, and used; and (iii) a written release executed by the Data Subject, which may be evidenced by an electronic signature as permitted under 740 ILCS 14/10.

(d) "**BIPA Retention Policy**" means a publicly available written policy establishing a retention schedule and guidelines for permanently destroying Biometric Data when the initial purpose for collection has been satisfied or within three (3) years of the Data Subject's last interaction with the relevant party, whichever occurs first, as required by 740 ILCS 14/15(a).

13.3 **Customer BIPA Obligations.** As the entity with a direct employment or contractual relationship with Data Subjects, Customer shall, prior to the activation or use of any Biometric Feature for any Data Subject, and throughout the term of this DPA:

(a) obtain a valid BIPA Written Release from each Data Subject prior to any Illinois Biometric Processing relating to that Data Subject, and maintain executed BIPA Written Releases in retrievable form for a minimum of three (3) years from the last date of Illinois Biometric Processing or the Data Subject's last interaction with Customer, whichever is later;

(b) adopt, maintain, and make publicly available a BIPA Retention Policy applicable to Biometric Data collected or processed in connection with the Services;

(c) not direct or configure Synovia to activate any Biometric Feature for any Data Subject for whom Customer has not obtained a valid BIPA Written Release;

(d) notify Synovia in writing within five (5) business days upon becoming aware of any revocation or withdrawal of consent by a Data Subject, and promptly direct Synovia to cease Illinois Biometric Processing for such Data Subject; and

(e) upon Synovia's reasonable written request (and in no event more than once per calendar year absent cause), provide Synovia with reasonable documentation evidencing Customer's compliance with this Section 13.3, including a representative sample of executed BIPA Written Releases (with personal identifying information redacted) and evidence of Customer's published BIPA Retention Policy.

13.4 **Activation Certification.** Prior to Synovia activating any Biometric Feature for Customer's account, Synovia shall provide Customer with: (a) written notice identifying the applicable Biometric Feature and the categories of Biometric Data it collects, stores, or processes; (b) model BIPA Written Release language and a BIPA Retention Policy template for Customer's use and adaptation; and (c) a written certification form ("**Activation Certification**"). Synovia shall not activate any Biometric Feature until Customer has completed and returned the Activation Certification, in which Customer certifies that: (i) Customer has reviewed the BIPA requirements applicable to the Biometric Feature; (ii) Customer has implemented a BIPA Written Release process and has obtained, or will obtain prior to first processing, valid BIPA Written Releases from all applicable Data Subjects; (iii) Customer has adopted and published a BIPA Retention Policy; and (iv) Customer acknowledges its independent obligations as a private entity under BIPA. Synovia shall require Customer to complete and return a renewal Activation Certification no later than

twelve (12) months following initial activation. Synovia may suspend access to any Biometric Feature upon Customer's failure to timely provide any required Activation Certification.

13.5 **Synovia Processing Restrictions.** Synovia shall, with respect to Biometric Data processed in connection with the Services:

(a) process Biometric Data solely for the purposes necessary to provide the Services to Customer and not for any other commercial purpose;

(b) not sell, lease, trade, or otherwise profit from Biometric Data, and not use Biometric Data for advertising, marketing, or profiling purposes or disclose it to any data broker or third-party analytics provider;

(c) not disclose Biometric Data to any third party except to authorized Subprocessors in accordance with Section 5 of this DPA, to Customer or Customer's authorized personnel, as required by applicable law, subpoena, warrant, or court order, or with Customer's prior written consent; and

(d) store, transmit, and protect Biometric Data using the reasonable standard of care within the telematics industry and at a level no less protective than Synovia applies to its own most sensitive confidential information, including through encryption of Biometric Data in transit and at rest and role-based access controls limiting access to authorized personnel with a documented need.

13.6 **Retention and Destruction of Biometric Data.** Synovia shall retain Biometric Data only for so long as is necessary to fulfill the applicable Service purpose and in no event longer than the period specified in Customer's BIPA Retention Policy communicated to Synovia in writing, or three (3) years from the last date of Illinois Biometric Processing for the applicable Data Subject, whichever is shorter. The deletion obligations set forth in Section 9 of this DPA shall apply to Biometric Data; for the avoidance of doubt, Synovia shall permanently and irreversibly destroy all Biometric Data within the timeframe specified in Section 9.1 and shall provide the written certification required by Section 9.2. Upon Customer's written request identifying a specific Data Subject, Synovia shall permanently delete all Biometric Data attributable to that Data Subject within thirty (30) days and shall confirm deletion in writing to Customer.

13.7 **Biometric Data Incident Notice.** In addition to the Personal Data Breach obligations set forth in Section 7 of this DPA, Synovia shall notify Customer without undue delay, and in no event later than seventy-two (72) hours after discovery, of any actual or reasonably suspected unauthorized access, acquisition, use, disclosure, or destruction of Biometric Data ("**Biometric Incident**"). Notice shall include, to the extent known: (a) a description of the nature of the Biometric Incident; (b) the categories and approximate volume of Biometric Data affected; (c) the categories and approximate number of Data Subjects affected; and (d) the measures Synovia has taken or proposes to take to address the Biometric Incident. Synovia shall cooperate with Customer in investigating and remediating any Biometric Incident and in satisfying any applicable notification obligations to Data Subjects or regulatory authorities.

13.8 **Indemnification.** Customer shall defend, indemnify, and hold harmless Synovia and its officers, directors, employees, and successors from and against any third-party claims, losses, damages, fines, penalties, and reasonable attorneys' fees arising out of or relating to: (a) Customer's failure to obtain valid BIPA Written Releases from any Data Subject prior to Illinois Biometric Processing; (b) Customer's failure to adopt, publish, or adhere to a BIPA Retention Policy; (c) Customer's material breach of any obligation under Section 13.3 of this DPA; or (d) Customer's use of Biometric Features for purposes beyond those disclosed in the applicable BIPA Written Release. Synovia shall defend, indemnify, and hold harmless Customer from and against any third-party claims arising out of or relating to: (i) Synovia's material breach of its obligations under Sections 13.5 or 13.6; or (ii) Synovia's unauthorized use, sale, or disclosure of Biometric Data in violation of this Section 13. Each Party's indemnification obligations under this Section 13.8 are conditioned upon the indemnified party providing prompt written notice, granting the indemnifying party sole control over defense and settlement (provided no settlement imposes liability on the indemnified party without its consent), and providing reasonable cooperation. The indemnification obligations in this Section 13.8 are subject to the limitations of liability set forth in the Principal Agreement.

13.9 **Representations.** Synovia represents and warrants that: (a) Synovia does not sell or commercially exploit Biometric Data; (b) Synovia's Biometric Features are designed and configured to activate only upon receipt of a completed Activation Certification from Customer; and (c) Synovia has implemented and maintains technical and organizational measures appropriate to protect Biometric Data against unauthorized access, acquisition, or disclosure. Customer represents and warrants that, as of each date on which Customer activates or uses a Biometric Feature: (i) Customer has obtained or will obtain, prior to first processing, valid BIPA Written Releases from all applicable Data Subjects; (ii) Customer has adopted and published a BIPA Retention Policy; and (iii) Customer's Activation Certification, when submitted, is complete and accurate.

14. **Order of Precedence**. The provisions of this DPA are supplemental to the provisions of the Principal Agreement. In the event of inconsistencies between the provisions of this DPA and the provisions of the Principal Agreement, the provisions of this DPA shall prevail.