UNCONTROLLED COPY – WEBSITE VERSION GOVERNS

Data Processing Agreement

This Data Processing Agreement (**"DPA"**) forms part of and is incorporated into Agreement between Customer and Provider and applies solely to Provider's Processing of Personal Data on behalf of Customer in connection with the Services (the **"Agreement"**). Capitalized terms not defined herein have the meanings set forth in the Agreement.

1. Parties; Incorporation; Scope

1.1 Parties. This DPA is entered into between: (i) the Customer entity identified in the Agreement (**"Customer"**) and (ii) the Provider entity identified in the Agreement . Each may be referred to as a "**Party"** and together, the **"Parties."**

1.2 Incorporation; Order of Precedence. This DPA is incorporated by reference into and forms part of the Agreement. In the event of any conflict between this DPA and the Agreement regarding the Processing of Personal Data, this DPA will control. If and to the extent the Standard Contractual Clauses (as defined below) apply, they will control over this DPA to the extent of any conflict.

1.3 Scope. This DPA applies only to the Processing of Personal Data by Provider as Processor (or "service provider/processor" under U.S. State Privacy Laws) on behalf of Customer as Controller (or "business"). This DPA does not govern the Parties' respective rights and obligations regarding: (a) Service Data (as defined below), except to the extent Service Data constitutes Personal Data processed on Customer's behalf; (b) Derived Data (as defined below), which is not Personal Data; or (c) Equipment/Telemetry Data that is not Personal Data, which is addressed in Annex IV and/or the Agreement.

1.4 Coverage of Affiliates.

(a) **Provider Affiliates.** Provider Affiliates may Process Personal Data on Provider's behalf. Provider Affiliates that Process Personal Data on behalf of Provider are deemed Subprocessors and are subject to the obligations of this DPA.

(b) **Customer Affiliates.** Customer Affiliates may use the Services only if expressly authorized in the Agreement (e.g., Order Form/SOW or schedule). Each such Customer Affiliate will be deemed a separate Controller with respect to its own Personal Data.

1.5 Term. This DPA remains in effect for the duration of Provider's Processing of Personal Data on behalf of Customer and until Provider has completed its obligations under **Section 12 (Return and Deletion)**.

2. Definitions

For purposes of this DPA:

2.1 "Affiliate" means any entity controlling, controlled by, or under common control with a Party, where "control" means ownership of greater than 50% of voting interests or equivalent power to direct management.

2.2 "(Applicable) Data Protection Laws" means all data protection, privacy, and security laws and regulations applicable to Provider's Processing of Personal Data under the Agreement, including, where applicable, (i) the European Union General Data Protection Regulation ("**GDPR**"), (ii) the UK GDPR and the UK Data Protection Act; (iii) the Swiss Federal Act on Data Protection; and (iv) U.S. state privacy laws, including the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA/CPRA**"), and other similar U.S. state laws (collectively, "**U.S. State Privacy Laws**").

2.3 "Customer Data" means data submitted to or generated in the Services by or for Customer, including Personal Data and Equipment/Telemetry Data to the extent provided or controlled by Customer. Customer Data excludes Service Data or Derived Data.

2.4 "De-identified Data" means data that has been de-identified or anonymized such that it cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person. De-identified Data is not Personal Data. Provider will maintain and apply measures designed to prevent re-identification and will not attempt to re-identify De-identified Data.

2.5 "(**Data) Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, as defined under the GDPR. The term "Controller" is used in this DPA solely for purposes of describing the Parties' roles under applicable Data Protection Laws and is intended to encompass functionally equivalent concepts (such as "business") under other applicable legal regimes, without expanding or modifying the obligations set forth in this DPA or the Agreement.

2.6 "(**Data) Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller, as defined under the GDPR. The term "Processor" is used in this DPA solely for describing the Parties'

roles and is intended to encompass functionally equivalent concepts (such as "service provider" or "processor") under other applicable Data Privacy Laws, without expanding or modifying the obligations set forth in this DPA or the Agreement.

2.7 "Derived Data" means aggregated and de-identified analyses, statistics, models, benchmarks, learnings, or insights generated by Provider from Processing of Customer Data and/or Service Data in connection with operating, securing, and improving the Services, provided Derived Data does not identify Customer or any data subject.

2.8 "Equipment/Telemetry Data" means machine-generated data from connected devices, sensors, controllers, building systems, transportation refrigeration units (TRUs), refrigerated containers and trailers, and other telematics endpoints. Equipment/Telemetry Data constitutes Personal Data only to the extent it is reasonably linkable to an identified or identifiable natural person (for example, operator/driver IDs or precise geolocation tied to a specific individual).

2.9 "Personal Data" means any information relating to an identified or identifiable natural person that is Processed by Provider on behalf of Customer under the Agreement, including "personal information" or "personal data" as defined in Applicable Data Protection Laws.

2.10 "Process" / "Processing" means any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, alignment, combination, restriction, erasure, or destruction.

2.11 "Security Incident" means a confirmed breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

2.12 "Service Data" means operational data relating to the provision, access to, and use of the Services (e.g., logs, event data, request metadata, performance metrics, and system telemetry), excluding Customer Data and Derived Data.

2.13 "Subprocessor" means any third party, including any Provider Affiliate, engaged by or on behalf of Provider to process Personal Data on Provider's behalf.

2.14 "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Commission Implementing Decision (EU).

2.15 "UK Addendum" means the UK International Data Transfer Addendum to the SCCs (or any successor recognized under UK law).

2.16 "Swiss Addendum" means the modifications/adaptations required for the SCCs to comply with Swiss data protection law and guidance of the Swiss FDPIC.

3. Roles; Customer Instructions; Purpose Limitation

3.1 Roles. For purposes of this DPA and the Processing of Personal Data under the Agreement, Customer is the Data Controller (or where applicable under U.S. State Privacy Laws, the "business"); Provider is the Data Processor (or, where applicable, the "service provider" or "processor"), solely with respect to Personal Data processed on Customer's behalf in accordance with under this DPA.

3.2 Documented Instructions. Provider shall process Personal Data solely in accordance with Customer's documented instructions as set forth in: (a) the Agreement, (b) this DPA (including its Annexes), and (c) Customer's lawful configurations and written directions issued by Customer's authorized representatives, and only for the purposes of providing, operating, maintaining, securing, and supporting the Services and complying with applicable law.

3.3 Instruction Legality. Provider shall promptly inform Customer if Provider reasonably believes that an instruction violates Applicable Data Protection Laws. Provider is not required to comply with an instruction that is unlawful or would cause Provider to violate Applicable Data Protection Laws.

3.4 Permitted Essential Processing. Notwithstanding Section 3.2, Provider may Process limited Personal Data as necessary to: (i) ensure security and integrity of the Services; (ii) prevent, detect, and remediate fraud, abuse, or misuse; (iii) debug and repair errors; (iv) provide billing, account administration and support; and (v) or comply with applicable legal obligations, in each case consistent with Applicable Data Protection Laws.

3.5 Prohibited Data; Special Categories; Children. Unless expressly agreed in writing with appropriate safeguards (e.g., in a Product Appendix and/or Order Form/SOW): (a) the Services are not designed to Process special categories of Personal Data or sensitive data requiring heightened protection (e.g., health/medical subject to HIPAA, payment card data subject to PCI DSS, biometric identifiers for identification, precise government IDs, or criminal offense data); and (b) the Services are not direct to children and are not designed to Process children's Personal Data. Customer will not submit such data to the Services absent written agreement. If Provider becomes aware that prohibited data has been submitted, Provider will notify Customer and delete or return such data as instructed unless retention is required by law.

3.6 Data Minimization. Provider will limit Processing to Personal Data reasonably necessary for the instructed purposes and will support correction/deletion actions initiated by Customer using available Service functionality.

4. Confidentiality

4.1 Confidentiality Obligations. Provider will ensure that all persons authorized to Process Personal Data are subject to binding confidentiality obligations no less protective than those set forth in the Agreement. Provider shall limit access to Personal Data to personnel with a strict need-to-know, periodically review access rights, promptly revoke access when no longer required, and provide appropriate privacy and security training.

4.2 **Non-Personal Customer Data.** For avoidance of doubt, confidentiality obligations applicable to Customer Data that is not Personal Data are governed by the Agreement.

5. Security Measures (Technical and Organizational Measures)

5.1 TOMs. Provider shall implement and maintain appropriate technical and organizational measures (**"TOMs"**) designed to protect Personal Data against unauthorized or unlawful processing and accidental loss, destruction, or damage, as described in **Annex II.**

5.2 Risk-Based Program; Variance by Offering. Provider maintains a documented, risk-based information security program appropriate to the nature of the Services. Because Provider's offerings, hosting environments, and third-party dependencies vary, the specific control implementations and security evidence (e.g., reports, certifications, summaries) may vary by offering; however, Provider will maintain an overall level of protection appropriate to the risk.

5.3 Updates. Provider may update TOMs from time to time to maintain or improve security and compliance, provided the overall level of protection is not materially diminished.

6. Security Incidents

6.1 Notification. Provider shall notify Customer without undue delay and in any event within seventy two (72) hours after confirmation of a Security Incident affecting Customer Personal Data. Where Provider reasonably suspects a material incident may involve Customer Personal Data and early notice is needed for Customer to meet legal obligations, Provider will provide notice consistent with this Section.

6.2 Contents. Notice will include, to the extent known at the time: (i) the nature of the Security Incident, (ii) the categories and approximate number of affected data subjects and records; (iii) likely consequences; (iv) measures taken or proposed to address the Security Incident and mitigate adverse effects; and (v) a point of contact.

6.3 Investigation; Mitigation & Cooperation. Provider will investigate the Security Incident, take reasonable steps to remediate, and document corrective actions. Provider will reasonably cooperate with Customer's reasonable instructions regarding the Security Incident, except where prohibited by law, not technically feasible, would compromise security, or would adversely affect other customers. For multi-customer incidents, Provider

may coordinate response and limit disclosures to what is reasonably necessary and appropriate in light of confidentiality, security, and legal constraints.

7. Subprocessor

7.1 General Authorization; List. Customer authorizes Provider to engage Subprocessors to Process Personal Data on Provider's behalf

7.2 Subprocessor List URL; Notice. Provider will maintain an up-to-date list of Subprocessor (via URL or schedule) identifying each Subprocessor's name, role, processing activities and location(s). Provider will provide at least thirty (30) days' prior notice of additions or replacements by updating the Subprocessor List URL and providing notice to Customer via email or other method specified in the Agreement's notice provisions.

7.3 Objection Right. Customer may reasonably object to a new Subprocessor by notifying Processor promptly in writing, stating reasonable grounds, within ten (10) business days after receipt of notice. If Customer objects, Processor will use commercially reasonable efforts to provide a reasonable workaround to avoid the Subprocessor's Processing of Customer Personal Data. If no workaround is available within thirty (30) days, either Party may terminate the affected Services without penalty (and any refunds, if applicable, will be handled in accordance with the Agreement).

7.4 Flow-down; Liability. Provider will impose on each Subprocessor obligations no less protective than those set out in this DPA. Provider remains responsible for the acts and omissions of its Subprocessors in connection with this DPA.

7.5 Third-Party Service Boundary. Certain modules may be "Third-Party Services" under the Agreement and may involve third-party platforms/networks outside Provider's direct control. Such third parties are treated as Subprocessors only to the extent they Process Personal Data on Provider's behalf. Otherwise, Customer's use of Third-Party Services is governed by the Agreement, the applicable Product Appendix, and any applicable Third-Party Provider Terms.

8. Assistance; Data Subject Rights; DPIAs; Regulatory Requests

8.1 Data Subject Requests (DSARs). Taking into account the nature of Processing, Provider will provide reasonable assistance (including appropriate technical and organizational measures, where feasible) to enable Customer to respond to data subject requests under Applicable Data Protection Laws (e.g., access, correction, deletion, restriction, portability, objection, and applicable U.S. opt outs). Provider will not respond to a data subject request directly unless legally required or authorized by Customer. Customer is responsible for verifying the requester's identity and for communications with data subjects unless Customer authorizes Provider in writing to respond.

8.2 GDPR/UK GDPR Articles 32-26. Provider will provide reasonable assistance to Customer to support Customer's compliance with obligations under GDPR/UK GDPR Articles 32-36 (security, breach notification support, DPIAs, and prior consultation), considering the nature of the Services and the information available to Provider.

8.3 Compelled Disclosures. If Provider receives a legally binding request from a governmental authority for Personal Data or Customer Data processed on Customer's behalf, Provider shall:

(a) assess whether the request is valid and enforceable under Applicable Data Protection Laws, including GDPR Article 48 where applicable;

(b) challenge or seek to narrow the request where there are reasonable grounds to do so, including where the request conflicts with Applicable Data Protection Laws;

(c) notify Customer without undue delay prior to disclosure, unless prohibited by law;

(d) disclose only the minimum data required, and only after exhausting available legal remedies; and

(e) where disclosure is required notwithstanding conflict, document the legal basis and scope of disclosure.

Nothing in this Section requires Provider to violate applicable law, nor does it obligate Provider to challenge a request where doing so would be unlawful, futile, or disproportionate in light of the circumstances.

8.4 Proportionality; Fees. Provider's assistance obligations are limited to assistance that is commercially reasonable and proportionate to the nature of the Processing and Services. If Customer requests assistance that materially exceeds standard support associated with the Services, Provider may charge reasonable fees upon prior notice and mutual agreement on scope.

8.5 Switching Assistance. For avoidance of doubt, switching and transition assistance (including post-termination export support) is governed by the Agreement, except as expressly stated in this DPA for Personal Data return/deletion.

9. International Data Transfers

9.1 Transfer Mechanisms. Where Provider or its Subprocessors transfer Personal Data from the EEA, UK, or Switzerland to a country not recognized as providing adequate protection, the Parties will rely on: (a) SCCs (EU 2021/914) (Module as applicable); (b) the UK Addendum for UK transfers; and (c) the Swiss Addendum for Swiss transfers. The SCCs and applicable Addenda are incorporated by reference, and completed by **Annex I** (details) and **Annex II** (TOMs). Any disclosure of Personal Data pursuant to a request from a non-EEA

governmental authority shall be subject to Section 8.3 and shall be made only in accordance with GDPR Article 48, the SCCs, and Applicable Data Protection Laws.

9.2 SCC Model Selection

(a) Controller-to-Processor transfers: Module 2 applies

(b) Processor-to-Processor onward transfers (where applicable): **Module 3** applies.

9.3 SCC Elections (Standard Positions). To the extent permitted by Applicable Data Protection Laws:

(a) **Clause 7 (Docking)**: does not apply.

(b) **Clause 9**: Option 2 (general written authorization) applies; notice period is as set out in **Section 7.2**.

(c) **Clause 11**: optional independent dispute resolution language does not apply.

(d) **Clause 17 (Governing law)** and **Clause 18 (Forum)**: the Parties select the law and forum of an EU Member State that permits the SCCs, designated by Provider for the relevant transfer (which may be Germany and the courts of Frankfurt am Main, unless otherwise required by Applicable Data Protection Laws or a competent supervisory authority).

9.4 Intra-Group Transfers Under BCRs. For Personal Data transfers to Provider's Affiliates that are covered by the Carrier Binding Corporate Rules (**"BCRs"**), such transfers shall be made in accordance with the BCRs. The BCRs are available at: https://corporate.carrier.com/BCR. This subsection applies only to intra-group transfers to Provider Affiliates included within the scope of the approved BCRs and does not limit or replace the transfer mechanisms set out in Section 9.1 for transfers to other recipients.

10. Audits; Compliance Evidence

10.1 Compliance Evidence. Provider shall make available to Customer, upon request and subject to confidentiality, reasonable information necessary to demonstrate compliance with this DPA, which may include applicable third-party audit reports or certifications (if maintained for the relevant offering), security summaries, and/or responses to reasonable security questionnaires.

10.2 Audit Rights. Customer may conduct a targeted audit of Provider's compliance with this DPA no more than once per year upon at least thirty (30) days' prior written notice, during business hours, and subject to confidentiality and minimal disruption to Provider's operations. Onsite audits are permitted only where the compliance evidence provided does not reasonably address documented compliance concerns, or following a material Security Incident where audit is reasonably necessary to verify remediation.

10.3 Restrictions; No Security Testing Rights Granted. Nothing in this DPA grants Customer any right to perform penetration testing, vulnerability scanning, or other security testing of the Services except as expressly permitted in writing by Provider in accordance with the Agreement.

10.4 Costs. Each party bears its own costs in connection with an audit, except that if an audit reveals material non-compliance with this DPA, Provider will reimburse Customer for reasonable, documented audit costs. Provider may charge reasonable fees for extraordinary audit requests upon prior notice and agreement.

11. Records; Demonstration of Compliance

Provider will maintain records of Processing activities to the extent required by Applicable Data Protection Laws and will make available information reasonably necessary to demonstrate compliance with this DPA as set forth in Section 10.

12. Return and Deletion

12.1 Return/Deletion Upon Termination. Upon termination or expiration of the Services, Provider will, at Customer's option, return or delete Customer Personal Data in Provider's possession or control, except to the extent retention is required by law.

12.2 Sequencing with Post-Termination Export. Where the Agreement provides a post-termination export period for Customer Data, Provider will not delete Customer Personal Data needed for such export until the earlier of (i) completion of the export requested by Customer in accordance with the Agreement, or (ii) expiration of the applicable export period, after which Provider will proceed with return/deletion in accordance with this Section 12.

12.3 Timing. Provider will complete return/deletion within a commercially reasonable timeframe, generally within ninety (90) days after the deletion trigger described in Sections 12.1-12.2, unless the Parties agree otherwise in writing or longer retention is required by law.

12.4 Backups and Logs. Customer Personal Data may remain in backups and disaster recovery systems until overwritten in accordance with Provider's standard retention cycles and in security logs/audit trails maintained for security and compliance. Any retained data remains subject to appropriate security and confidentiality and will not be accessed except as required for permitted purposes.

12.5 Subprocessors. Provider will ensure Subprocessors delete or return Customer Personal Data consistent with this Section 12 upon termination of their subprocessing.

13. U.S. State Privacy Laws (Including CCPA/CPRA)

To the extent U.S. State Privacy Laws apply to Provider's Processing of Personal Data under the Agreement:

13.1 Service Provider/Processor Commitments. Provider will:

(a) Process Personal Data solely to perform the Services and the business purposes described in the Agreement and this DPA (including security, integrity, debugging, fraud prevention, account administration, and compliance);

(b) not "sell" or "share" Personal Data (as those terms are defined under CCPA/CPRA) and not Process Personal Data for cross-context behavioral advertising;

(c) not retain, use, or disclose Personal Data outside the direct business relationship with Customer except as permitted by Applicable Data Protection Laws;

(d) not combine Personal Data with personal data received from other sources except as permitted for service providers/processors (including to maintain or improve the Services using De-identified and/or aggregated outputs) and as otherwise permitted by law;

(e) flow down the restrictions in this Section 13 to its Subprocessors; and

(f) provide the same level of privacy protection for Personal Data as required under Applicable Data Protection Laws for the Processing in scope.

13.2 Customer Disclosures. Customer discloses Personal Data to Provider solely for the limited and specified purposes set forth in the Agreement and this DPA.

14. Customer Responsibilities.

Customer is responsible for:

(a) establishing a lawful basis for Processing and providing required notices and obtaining consents where required;

(b) ensuring that its instructions are lawful and do not cause Provider to violate Applicable Data Protection Laws;

(c) configuring and using the Services appropriately, including managing access controls, user permissions, credentials, and any geolocation/retention settings provided in the Services;

(d) ensuring Personal Data submitted is accurate, up to date, and limited to what is necessary; and

(e) ensuring it does not submit prohibited data except as expressly agreed in writing with appropriate safeguards.

15. Miscellaneous

15.1 Limitation of Liability. The limitations and exclusions of liability set forth in the Agreement apply to this DPA to the maximum extent permitted by law.

15.2 Changes to This DPA. Provider may update this DPA (including its Annexes) from time to time to reflect changes in the Services, Subprocessors, or Applicable Data Protection Laws. Provider will post the updated DPA and will indicate the effective date. Material changes will not apply retroactively and will become effective thirty (30) days after posting, unless required sooner to comply with Applicable Data Protection Laws. Customer's continued use of the Services after the effective date constitutes acceptance of the updated DPA. Notwithstanding the foregoing, Provider may update the Subprocessor List URL as described in Section 7.2.

15.3 Severability. If any provision of this DPA is held invalid or unenforceable, the remaining provisions will remain in full force and effect.

15.4 No Third-Party Beneficiaries. Except as expressly provided in the SCCs (where applicable), this DPA does not confer any rights or remedies on any third party.

15.5 Conflicting Legal Obligations. Where compliance with Customer's instructions or Provider's obligations under this DPA would cause Provider to violate applicable law (including data protection, cybersecurity, state secrecy, or data localization laws), Provider shall be excused from performance to the extent of the conflict and shall promptly notify Customer. The Parties shall cooperate in good faith to implement a lawful alternative that preserves, to the extent reasonably practicable, the intended purpose of the Processing.

ANNEX I - Details of Processing (SCC Annex I)

A List of Parties and Roles

Data Exporter (Controller): Customer (and authorized Customer Affiliates identified in the Agreement, if any)
Data Importer (Processor): Provider (and its Subprocessors listed at the Subprocessor List URL)

B. Description of the Transfer / Processing

1) Categories of data subjects. Customer employees, contractors, administrators, field technicians/service personnel, drivers/operators (where applicable), and other authorized end users of the Services.

2) Categories of Personal Data. Depending on the Services and Customer's configuration, may include:

- account identifiers and contact details (name, business email, phone, username);
- authentication data and access/role/permission information;
- identifiers associated with devices/equipment/telematics endpoints, to the extent linkable to individuals;
- audit logs, event logs, and alarm logs attributable to a user/account;
- geolocation/route data where linked to an identifiable individual (e.g., driver/operator identifier);
- support case data and ticket metadata; and
- free text fields entered by Customer users (excluding special categories of Personal Data, which are not applicable unless expressly agreed in writing).

3) Special categories / sensitive data. Not applicable.

4) Nature of Processing. Collection, recording, organization, structuring, storage, hosting, retrieval, consultation, use, disclosure by transmission (to authorized users and Subprocessors), alignment/combination as instructed, restriction, and deletion/return.

5) Purposes of Processing. Provide, operate, maintain, secure, and support the Services; perform Customer's documented instructions; prevent fraud and misuse; ensure service integrity; provide billing/account administration; and comply with law. Product improvement and analytics occur via De-identified and/or aggregated outputs as permitted by the Agreement and this DPA.

6) Frequency of transfers. Continuous and/or periodic, depending on Service use.

7) Duration of Processing / retention. For the term of the Agreement, plus any transition/export period described in the Agreement, and thereafter until completion of return/deletion obligations under Section 12, subject to permitted backup/log retention.

C. Competent supervisory authority

As determined under GDPR/UK GDPR/Swiss law and the SCCs/Addenda, as applicable.

ANNEX II - Technical and Organizational Measures (SCC Annex II)

Provider maintains a documented, risk-based information security program appropriate to the Services, including measures such as:

1. **Governance & Risk:** security policies; risk assessments; asset management; training; third-party risk management.
2. **Access Controls:** least privilege; role-based access; unique IDs; MFA for administrative access where supported; periodic access reviews; secure credential practices.
3. **Encryption & Keys:** encryption in transit and at rest where appropriate; secure key management with restricted access and appropriate operational controls.
4. **Secure Development:** secure SDLC practices appropriate to the offering, such as code review, change control, and vulnerability management.
5. **Monitoring & Logging:** logging/monitoring appropriate to detect unauthorized access; incident response procedures.
6. **Vulnerability Management:** processes to identify, triage, and remediate vulnerabilities based on risk and severity.
7. **BC/DR:** backup and recovery processes appropriate to the offering.
8. **Physical Security:** physical security controls for facilities/data centers used to host the Services (as applicable).
9. **Subprocessor Security:** contractual security obligations and diligence appropriate to Subprocessor role.

Security evidence. Subject to confidentiality, Provider will provide reasonable evidence of security controls for in-scope offerings upon request, which may include third-party reports/certifications (if maintained), executive summaries, and/or questionnaire responses.

ANNEX III - Subprocessors

Provider maintains an uptodate list of Subprocessors authorized to process Personal Data on Provider's behalf, available upon request, and provides advance notice of material changes in accordance with Section 7.

ANNEX IV – Equipment/Telemetry & Derived Data Governance (Non-Personal Data)

This Annex governs **Equipment/Telemetry Data that does not constitute Personal Data**. If Equipment/Telemetry Data becomes Personal Data (i.e., is reasonably linkable to an individual), the body of this DPA and Annex I apply.

1) Permitted Processing. Provider may Process non-Personal Equipment/Telemetry Data for diagnostics, monitoring, analytics, predictive maintenance, optimization, benchmarking, security, and improvement of the Services.

2) Rights and Derived Data. Customer retains rights in raw non-Personal Equipment/Telemetry Data it provides or controls. Provider may create, use, and own Derived Data, provided Derived Data does not identify Customer or any individual and does not include Customer Confidential Information.

3) EU Data Act. To the extent the European Union Data Act applies, Customer shall be deemed the "user" of the connected products and related services for purposes of exercising statutory access and portability rights, unless otherwise specified in an applicable Order Form or Product Appendix. Provider shall support Customer's legally required access to and portability of non-personal or mixed Equipment/Telemetry Data generated through Customer's use of the Services using standard technical means appropriate to the relevant offering. This provision does not expand Provider's obligations with respect to Personal Data, which remain governed exclusively by the body of this DPA.

4) No Re-identification. Provider will not attempt to re-identify any individual from non-Personal Equipment/Telemetry Data or Derived Data and will maintain safeguards designed to prevent re-identification.

5) Retention. Non-Personal Equipment/Telemetry Data will be retained in accordance with service requirements, regulatory obligations, and Provider's standard operational retention schedules.