Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms an integral part of the services Agreement (the "**Agreement**") entered into by and between the Customer approving this DPA, (hereinafter referred to as "**Customer**") and **Kornit** or any of its affiliates (hereinafter referred to as "**Processor**") and shall, upon execution, be deemed to be incorporated into and form part of the Agreement.

References herein to "you" and "your" shall mean the Customer.

Customer and Processor are hereinafter jointly referred to as the "**Parties**" and individually as the "**Party**". Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

1. **Definitions.** In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth opposite each one of them:

1.1. "**Affiliate**" means an entity that, directly or indirectly, owns or controls, is owned or is controlled by, or is under common ownership or control with a party. As used herein, “control” means the power to direct the management or affairs of an entity and “ownership” means the beneficial ownership of more than fifty percent (50%) of the voting equity securities or other equivalent voting interests of an entity

1.2. **"Controller"** means an entity which, alone or jointly with others, determines the purposes and means of the processing of the Personal Data

1.3. "**Customer Personal Data**" means any Personal Data Processed by Processor on behalf of Customer pursuant to or in connection with the Agreement; including historical operational data and user account data transferred during tenant consolidation

1.4. "**Data Protection Laws**" means applicable data protection and privacy laws of any country, including but not limited to the EU Data Protection Laws, UK GDPR, the California Consumer Protection Act and California Privacy Rights Act (CCPA/CPRA), Australian Privacy Act 1988 (Cth), Canadian PIPEDA / Quebec Law 25, Mexican LFPDPPP, and, to the extent applicable, the data protection or privacy laws of any other applicable country as agreed in writing between the Parties;

1.5. "**Data Subject**" means an identified or identifiable natural person who can be identified, directly or indirectly, by reference to an identifier;

1.6. "**EU Data Protection Laws**" means EU General Data Protection Regulation 2016/679 ("GDPR"), as amended, replaced or superseded from time to time, laws implementing or supplementing the GDPR, and any other laws and regulations of the EU and its Member States applicable to the protection of Personal Data;

1.7. "**Personal Data**" means any information relating to an identified or identifiable Data Subject; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

1.8. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

1.9. "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.10. "**Subprocessor**" means any person (including any third party and any Processor Affiliate, but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor to Process Personal Data on behalf of the Customer in connection with the Agreement; and

1.11. "**Standard Contractual Clauses**" means the MODULE TWO: Transfer controller to processor of the contractual clauses set out in the Annex of European Commission Decision 2021/915 and available at https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN which are incorporated into this Agreement by way of reference and made an integral part hereof, where the following options will apply: option 2 of Section 9 with fourteen (14) days as the applicable notice period, option 1 of Section 17 with Germany as the governing law, and courts of Düsseldorf in Section 18(b); and

2. **Processing of Customer Personal Data.**

2.1. **Authority:** Customer warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in Section 2.3 on behalf of each relevant Customer Affiliate.

2.2. **Scope of Processing:** Processor shall not Process Customer Personal Data other than on the Customer's written instructions set in Section 2.3 below (including for purposes of the Agreement and execution of multi-tenant consolidation), unless Processing is otherwise required by Applicable Laws to which the Processor is subject.

2.3. **Customer Instructions**: Customer instructs Processor (and authorizes Processor to instruct each Subprocessor) to (i) Process Customer Personal Data; and (ii) in particular, transfer Customer Personal Data to any country or territory (including across Europe, Australia, Canada, Mexico, and North America), all as reasonably necessary for the provision of the Services and consistent with the Agreement and Privacy Policy (as defined under the Agreement) and in accordance with applicable Data Protection Laws.

2.4. Customer sets forth the details of the Processing of Customer Personal Data, in **Annex 1** (*Details of Processing of Customer Personal Data*), attached hereto.

3. **Controller Responsibilities:** End User Consent & Legal Basis: The Controller is solely responsible for determining the lawful basis for the processing of personal data under applicable data protection laws, including any user behavior tracking enabled through the Processor's platform. Where required by applicable law, including but not limited to in cases involving the tracking of end-user behavior or employee monitoring across regions, the Controller shall ensure that valid, informed consent or appropriate legal notices are obtained from data subjects prior to the collection, migration, or processing of their personal data. The Controller shall provide appropriate notices and obtain any necessary authorizations, consents, or approvals from data subjects to permit the Processor to process personal data in accordance with this Agreement and the Controller's documented instructions.

4. **Processor Personnel.** Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the 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 necessary for the purposes of the Agreement, and to comply with Applicable Laws, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. **Security.** 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. In assessing the appropriate level of

security, Processor shall take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

6. **Sub Processing**.

6.1. **Existing Subprocessors:** Processor and each Processor Affiliate may continue to use those Subprocessors already engaged by Processor or any Processor Affiliate as at the date of this DPA, subject to Processor and each Processor Affiliate in each case as soon as practicable meeting the obligations set out in Section 6.3.

6.2. **Objections & Termination**: Customer authorizes Processor and each Processor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this Section 6 to appoint) Subprocessors in accordance with this Section 5 and any restrictions in the Agreement. Upon request, Processor shall give Customer details of any Subprocessor, including relevant details of the Processing to be undertaken by the Subprocessor. If Customer notifies Processor in writing of any objections (on reasonable grounds) to any appointment of Subprocessor, Processor shall not appoint (or disclose any Customer Personal Data to) such Subprocessor until reasonable steps have been taken to address the reasonable objections raised by Customer. Where such steps are not sufficient to relieve Customer's reasonable objections then Processor may by written notice to Customer with immediate effect terminate the Agreement to the extent that it relates to the services which require the use of the proposed Subprocessor.

6.3. **Subprocessor Agreements:** With respect to each Subprocessor, Processor shall ensure that the arrangement between the Processor and the Subprocessor is governed by a written contract including terms which offer a similar level of protection for Customer Personal Data as those set out in this DPA and meet the requirements of Applicable Laws.

7. **Data Subject Rights**.

7.1. **Assistance**: Taking into account the nature of the Processing, Processor shall reasonably assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under Data Protection Laws, at Customer's sole expense.

7.2. **Direct Requests:** 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 it responds to the request.

8. **Personal Data Breach**.

8.1. **Notification**: Processor shall notify Customer without undue delay, and in any event within 72 hours, upon Processor or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects or Data Protection authorities of the Personal Data Breach under Data Protection Laws.

8.2. **Remediation**: Processor shall cooperate with Customer and take such commercially reasonable steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such

Personal Data Breach, at Customer's sole expense. Data Protection Impact Assessment and Prior Consultation.

8.3. Processor and each Processor Affiliate shall provide reasonable assistance, on Customer's expense, to Customer with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities, 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 Processor.

9. **Deletion or return of Customer Personal Data**.

9.1. **Return/Deletion Request**: Subject to Section 9.2, if requested by Customer in writing upon or in connection with the termination of the Agreement, Processor shall promptly and in any event within thirty (30) days of the date of cessation of any services involving the Processing of Customer Personal Data, delete or return all copies of Customer Personal Data, except such copies as required to be retained in accordance with applicable law and/or regulation.

9.2. **Legal Retention**: Processor may retain Customer Personal Data to the extent required by Data Protection Laws and only to the extent allowed by Applicable Laws and always provided that Processor shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10. **Audit Rights**

10.1. Subject to Sections 10.2 to 10.3, Processor shall make available to Customer, upon prior written request, electronic copies of all information necessary to reasonably demonstrate compliance with this DPA, and shall allow for and contribute to audits which may take place via assessment questionnaires, including inspections, by a reputable auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Processor, provided that such third-party auditor shall be subject to confidentiality obligations.

10.2. Provision of information and audits are at Customer's sole expense and only arise under Section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

10.3. Customer shall give Processor reasonable prior written notice of any audit or inspection to be conducted via assessment questionnaire under Section 10.1 and shall make (and ensure that each of its mandated auditors makes) endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Processors' systems, cloud environment, equipment, and business in the course of such an audit or inspection. Processor need not give access to its systems for the purposes of such an audit or inspection.

10.4. Customer shall not conduct more than one (1) audit or inspection, in respect of each Processor, in any calendar year, except for any additional audits or inspections which:

10.4.1. Controller reasonably considers necessary because of genuine concerns as to Processor's compliance with this DPA; or

10.4.2. Controller is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory; or

10.4.3. where Controller has identified its concerns or the relevant requirement or request in its prior written notice to Processor of the audit or inspection.

11. **Cross-border data transfers**

11.1. General Transfer Safeguards: If any Data Protection Laws include requirements to permit the cross-border transfer of Customer Personal Data, the Parties will comply with such requirements, including executing applicable Standard Contractual Clauses (SCCs), relying on applicable adequacy decisions, or executing alternative legitimate transfer mechanisms.

11.2. EU & Swiss Transfers: To the extent Customer Personal Data originating from the European Economic Area (EEA) or Switzerland is transferred outside those regions to a jurisdiction not recognized as providing an adequate level of data protection, the Standard Contractual Clauses (Module Two: Controller-to-Processor) set forth in European Commission Decision 2021/914 are hereby incorporated by reference and shall apply.

11.3. UK Transfers: To the extent Customer Personal Data is subject to UK Data Protection Laws, the Standard Contractual Clauses apply as amended by Part 2 of the UK International Data Transfer Addendum ("UK Addendum")[cite: 3, 4]. For the purposes of Part 1 of the UK Addendum: (a) the details of the parties are set out in the Agreement; (b) the selected modules and clauses correspond to Module Two of the Standard Contractual Clauses; (c) the appendix information is set out in Annex 1 of this DPA; and (d) the 'Exporter' is elected.

11.4. Australia, Canada & Mexico Transfers: To the extent Customer Personal Data originates from Australia, Canada, or Mexico and is transferred across borders (including during multi-region tenant consolidation), Processor agrees to afford a level of protection to Customer Personal Data comparable to the statutory requirements under the Australian Privacy Principles (APP 8), Canadian PIPEDA and Quebec Law 25, and Mexican LFPDPPP, respectively.

12. **General Terms**

12.1. **Governing Law and Jurisdiction**.

12.1.1. the Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.1.2. this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

12.2. **Order of Precedence**. Nothing in this DPA reduces Processor's obligations under the Agreement in relation to the protection of Personal Data or permits Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Privacy Policy (as defined under the Agreement), the Privacy Policy shall prevail provided only that the procedure prevailing through the Privacy Policy shall not constitute as a breach or infringement of any Applicable Laws.

12.3. Subject to Section 12.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other Agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) Agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

12.4. **Changes in Data Protection Laws**.

12.4.1. Customer may by at least thirty (30) calendar days' prior written notice to Processor, propose any other variations to this DPA, which are reasonably considered to be necessary to address the requirements of any Data Protection Law.

12.4.2. If Customer gives notice under Section 12.4.1, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

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

13. AI Features & Machine Learning Processing

13.1. Scope of AI Processing: To the extent Customer elects to utilize AI-powered platform features (including automated service agents, diagnostic support tools, predictive maintenance modules, and spare parts/inventory insights), Processor may Process Customer Personal Data and operational inputs solely to generate AI outputs and provide such features in accordance with Customer's instructions.

13.2. No Model Training on Personal Data: Processor warrants that Customer Personal Data provided into AI features (including user prompts, support agent transcripts, and technician inputs) shall not be used to train, retrain, fine-tune, or improve public, multi-tenant, or foundational third-party AI models without Customer's prior written consent.

13.3. Third-Party AI Subprocessors: Where AI features leverage specialized third-party infrastructure or models (e.g., cloud-hosted Large Language Models or specialized analytics engines), Processor shall ensure such entities operate as vetted Subprocessors bound by written terms no less restrictive than this DPA.

13.4. Anonymized Analytics: Processor may process aggregated, de-identified, or non-personal telemetry data (e.g., machine error codes, part usage patterns, system uptime statistics) to optimize predictive spare parts inventory and platform maintenance models, provided such data contains no Personal Data.

Annex 1: Details of Processing of Customer Personal Data

- **Categories of Personal Data:** Names, email addresses, login credentials, IP addresses, job titles, technician IDs, user interaction logs, platform activity history, support interaction logs, AI service agent queries, and spare parts diagnostic inputs.
- **Categories of Data Subjects:** Employees, contractors, operators, technicians, and platform users of Customer or Customer's Affiliates.
- **Nature & Purpose of Processing:** Cloud platform hosting, software provision, system administration, AI-driven service support, automated parts diagnostic insights, and optional multi-region tenant consolidation.
- **Retention Period:** Retained for the duration of the Agreement and returned/deleted in accordance with Section 6.1.