

Tennant
EULA Data Protection Addendum

This EULA Data Protection Addendum (the “**Addendum**” or “**DPA**”) is incorporated into and subject to the terms and conditions of the End User License Agreement for Autonomous Navigation Software between you (the “**End User**”) and the affiliate of Tennant Company referred to therein (“**Tennant**”) (the “**EULA**”); together the EULA and the Addendum shall be referred to herein as the “**Agreement**”).

1. **Defined Terms.** Capitalized terms used in this Addendum that are not otherwise defined herein will have the same meaning ascribed to them as set forth in the EULA.
 - a. “**Affiliate**” means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
 - b. “**BrainOS-enabled Robots**” means any robot containing the Software and provided under an active subscription under the EULA.
 - c. “**End User Personal Data**” means any Personal Data provided to Tennant or any of its Sub-processors by the End User employees, contractors, Permittees or other designated agents when utilizing Software of BrainOS-enabled Robots.
 - d. “**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.
 - e. “**Data Laws**” means data protection and privacy laws and regulations applicable to the Processing of Personal Data in any relevant jurisdiction.
 - f. “**Data Subject**” means the identified or identifiable person to whom End User Personal Data relates.
 - g. “**EEA**” means the European Economic Area.
 - h. “**European Data Laws**” means all applicable data protection and privacy laws and regulations in European jurisdictions, including, but not limited to, for EEA territories, the General Data Protection Regulation (EU) 2016/679 and any successor legislation and associated national implementations thereto (the “GDPR”) and, for the United Kingdom, the United Kingdom Data Protection Act 2018, and the Switzerland Federal Act on Data Protection.
 - i. “**Non-European Data Laws**” means all applicable data protection and privacy laws and regulations outside of European jurisdictions, including, but not limited to, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, Colorado Privacy Act of 2021, Connecticut Data Privacy Act, Utah Consumer Privacy Act of 2022, Virginia Consumer Data Protection Act of 2021, Montana Consumer Data Privacy Act, Texas Data Privacy and Security Act and Oregon Consumer Privacy Act.
 - j. “**Personal Data**” means any data or information that constitutes “personal data”, “personal information” or “personally identifiable information” under applicable Data Laws.
 - k. “**Process, Processed, and Processing**” means any operation or set of operations which is performed on End User Personal Data or on sets of End User Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
 - l. “**Processor**” means the entity which Processes Personal Data on behalf of the Controller.
 - m. “**Security Incident**” means, in connection with the Services, any unauthorized use, modification, loss, compromise, destruction or disclosure of or access to End User Personal Data.
 - n. “**Services**” means services provided by Tennant to the End User pursuant to the EULA, whether by itself or via a Sub-processor or any of other third-party.

- o. **“Standard Contractual Clauses” or “SCC”** means the standard contractual clauses that are a legally enforceable mechanism under Data Laws for the transfer of Personal Data to any country that does not have an adequate level of data protection to permit the transfer of Personal Data (pursuant to a decision of the relevant supervisory authority) (“Third Country”).
- p. **“Sub-processor”** means any third party that Tennant engages to assist with the provision of Services, which involves the Processing of End User Personal Data.
- q. **“Term”** means the duration of the active subscription under the EULA, together with any period of Unsupported Use.

2. **Processing of Data.**

- a. **Roles of the Parties.** The Parties acknowledge that with regard to the Processing of End User Personal Data in accordance with the Services, the End User is the Controller or “Business” (as such term is defined under Data Laws) and Tennant is the Processor or “Service Provider” (as such term is defined under Data Laws).
- b. **Processing of Personal Data.** Tennant and its Affiliates shall Process End User Personal Data in accordance with the End User’s documented written instructions. End User’s instructions shall not violate any applicable laws, including Data Laws. Tennant and its Affiliates shall Process End User Personal Data for the purposes, duration and other details set forth in **Appendix I**.
- c. **End User Compliance Obligations.** Without limiting the generality of this Section 2 (Processing of Data), the End User warrants that:
 - i. the End User shall have sole responsibility for the accuracy, quality, and legality of End User Personal Data and the means by which the End User acquired End User Personal Data, including receiving all consents, authorizations, and/or permissions necessary for Tennant and its Sub-processors to Process the End User Personal Data;
 - ii. the End User specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of End User Personal Data, to the extent applicable under Data Laws; and
 - iii. the End User has taken and further undertakes that throughout the Term it shall take all necessary steps (having regard to the nature of the circumstances in which End User Personal Data will be collected) to provide affected Data Subjects with an accurate, comprehensible, concise, conspicuous and easily accessible description of all processing of End User Personal Data carried out under and in connection with the Addendum, which are sufficient to meet the standards and requirements of Data Laws.

3. **Data Security.**

- a. **Tennant Security Measures.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing (as set forth in **Appendix I**) as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Tennant has implemented and maintains technical and organizational measures designed to protect End User Personal Data against Security Incidents as further described in **Appendix II**. Tennant may update or modify its respective security program from time to time, without notice to End User, provided that such updates and modifications do not materially decrease the overall security of the End User Personal Data.
- b. **Security Compliance by Tennant.** Tennant will grant access to End User Personal Data only to

employees, contractors, and Sub-processors who need such access for the scope of their performance and are subject to appropriate confidentiality arrangements.

- c. **Tenant Security Assistance.** Taking into account the nature of the Processing of End User Personal Data and the information available to Tennant, Tennant will provide the End User with commercially reasonable assistance necessary for the End User to comply with its obligations in respect of End User Personal Data under applicable Data Laws, and provided the End User shall reimburse Tennant for any such assistance.

4. **Security Incidents.**

- a. **Tenant's Obligations.** Tennant shall notify the End User by email and/or phone of any actual Security Incident without undue delay after becoming aware of such Incident. Tennant shall take reasonable steps to investigate the cause of such Security Incident, minimize harm to the End User, and prevent a recurrence of such Security Incident. Tennant will investigate any such Security Incident and take necessary steps to eliminate or contain the exposures that led to such Security Incident in accordance with Tennant's security program and applicable law. The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant data protection authorities.
- b. **End User's Obligations.** Other than agreeing on the content of related public statements or required notices, the End User is solely responsible for complying with incident notification laws applicable to the End User and fulfilling any third-party notification obligations related to any Security Incident(s). Tennant's notification of or response to a Security Incident will not be construed as an acknowledgement by Tennant or any of its Sub-processors of any fault or liability with respect to the Security Incident.

The End User agrees that, without prejudice to Tennant's obligations under this Section 4 (Security Incidents), the End User is solely responsible for its use of the Services, including:

- i. making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the End User Personal Data;
 - ii. securing the account authentication credentials, systems, and devices the End User uses to access the Services;
 - iii. securing the End User's systems and devices that Tennant and/or its applicable Sub-processors use to provide the Services; and
 - iv. backing up End User Personal Data.
5. **Audits.** Upon reasonable written request by End User, Tennant shall provide to the End User information necessary to reasonably demonstrate Tennant's compliance with this Addendum. Tennant evaluates, tests, and monitors the effectiveness of its security program and adjusts and/or updates its security program as reasonably warranted by the results of such evaluation, testing, and monitoring. In connection therewith, Tennant, from time to time, may also conduct an assessment of the implementation and maintenance of its security program and related compliance with both the Agreement and Data Laws ("**Audit Report**"). Upon the End User's reasonable request, Tennant shall provide a summary of its then-current Audit Report (to the extent such person has access to or handles End User Personal Data); provided, however, that the End User agrees that any such Audit Report shall be treated as confidential information of Tennant and the End User will not disclose it to third parties except for the End User's legal counsel and consultants bound by obligations of confidentiality.
6. **Legally Required Disclosures.** Tennant and its Sub-processors may disclose End User Personal Data and any other information about the End User to government or law enforcement officials or private parties if,

in their individual or joint reasonable discretion, they believe it is necessary or appropriate in order to respond to legal requests, demands, and orders, including subpoena, judicial, administrative, or arbitral orders of an executive or administrative agency, regulatory agency, or other governmental authority, to protect the safety, property, or rights of Tennant and/or such Sub-processors or of any other third party, to prevent or stop any illegal, unethical, or legally actionable activity, or to comply with applicable law. Except as otherwise required by applicable law, Tennant will notify the End User of any legal requests, demands, and orders that Tennant and/or any such Sub-processor receives, and that relate to the Processing of End User Personal Data.

7. Data Subject Rights.

- a. **End User’s Responsibility for Requests.** If Tennant receives a request from a Data Subject in relation to End User Personal Data, Tennant will advise the Data Subject to submit its request to the End User and the End User will be responsible for responding to any such request.
- b. **Data Subject Request Assistance.** Taking into account the nature of the Processing of End User Personal Data, Tennant will provide the End User with reasonable assistance as necessary for the End User to fulfill its obligation under Data Laws to respond to requests by Data Subjects to exercise their rights. The End User shall reimburse Tennant for any such assistance beyond providing self-service features included as part of the Services at Tennant’s then-current professional services rates, which shall be made available to the End User upon request.

8. Data Transfers Out of the EEA. If the storage and/or Processing of End User Personal Data occurs within the EEA, involves transfers of End User Personal Data out of the EEA or Switzerland, and the European Data Protection Legislation applies to the transfers of such data, Tennant will make such transfers in accordance with the SCCs.

9. Sub-processors. The End User acknowledges and agrees that Tennant may engage Sub-processors to Process End User Personal Data on the End User’s behalf. A list of approved Sub-processors of Tennant is set forth in **Appendix III**. The End User agrees that all such approved Sub-processors are permitted to Process End User Personal Data for the nature and purposes set forth herein. Tennant will maintain a list of Sub-processors as described in **Appendix III**. Tennant will update its website to reflect new Sub-processors within ten (10) calendar days prior to a Sub-processor beginning to Process End User Personal Data. The End User shall have ten (10) calendar days to reasonably object to the addition of any new Sub-processor. If the End User notifies Tennant in writing of any such objections, then Tennant and the End User shall negotiate in good faith and take reasonable steps to address the objections raised by the End User. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement with respect only to those Services which cannot be provided by Tennant without the use of the objected-to new Sub-processor by providing written notice to Tennant. Tennant shall require each Sub-processor to comply with contractual obligations no less onerous than Tennant’s obligations under this Addendum. Tennant shall oversee its Sub-processors to ensure that these contractual obligations are met.

10. Record Retention and Destruction. Tennant shall maintain records related to its Processing activities performed on behalf of the End User relating to End User Personal Data for at least the Term. Upon termination of this Agreement, Tennant shall delete any End User Personal Data in its possession, provided, however, that Tennant may retain a copy of any such End User Personal Data to the extent required by applicable law.

11. Notices. Notices required or permitted to be given to the End User hereunder may be provided to the End User’s primary point of contact with Tennant. Notices required or permitted to be given to Tennant hereunder may be provided by sending an email to privacy@tenantco.com. The End User is solely responsible for ensuring that such email address is valid.

12. Jurisdiction Specific Terms. To the extent Tennant Processes End User Personal Data originating from

and protected by Non-European Data Laws, then the terms specified in **Appendix IV** with respect to those applicable jurisdictions further apply in addition to the terms set forth herein. In the event of any conflict between such jurisdiction-specific terms and this Addendum, such jurisdiction-specific terms shall control.

- 13. Limitation of Liability.** Tennant’s and all of its Affiliates’ and Sub-processors’ liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the limitations of liability set forth in the EULA.
- 14. Effect of These Terms.** Except as otherwise set forth herein, the terms and conditions of this Addendum, including the Appendices, are part of and incorporated into the Agreement, and the terms and conditions of this Addendum constitute the entire and exclusive agreement between the parties with respect to its subject matter. To the extent of any conflict or inconsistency between this Addendum and the terms of the EULA, this Addendum will govern with respect to End User Personal Data.

[Appendices follow]

Appendix I – Processing Details

Subject Matter	The End User’s deployment on certain premises of the BrainOS-enabled Robots in connection with the general provision of the Services to the End User under and in accordance with the Agreement.
Duration of the Processing	The overall duration of Tennant’s Processing of End User Personal Data under the Agreement is the Term plus the period from the expiry of the Term until deletion of all End User Personal Data by Tennant in accordance with the Agreement.
Frequency of the Processing	On a continuous basis.
Nature and Purpose of the Processing	<p>Tennant will Process any such End User Personal Data for the following purposes:</p> <ul style="list-style-type: none"> i. Processing for supporting the Services, including provisioning, support, optimization and maintenance of the Services, including other Processing as set forth in the EULA. ii. Processing to comply with the End User’s instructions that are consistent with the Agreement, including, without limitation, communicating with the End User, handling support tickets and requests, and generally supporting the business relationship between Tennant and the End User. iii. Processing as set forth in and/or required by the EULA. iv. Creating and deriving anonymized and/or aggregated data related to use of the Services that does not identify the End User or any natural person, and use, publicize, or share such data with third parties to improve Tennant’s and/or Sub-processors’ products and services.
Categories of Data and Data Subjects	<p>The categories of data Processed by Tennant may include the business contact information of the End User employees, contractors, or other designated agents who use the Services which may include first name, last name, company email address, username, password, and mobile phone number (only to the extent End User uses a feature requiring this information).</p> <p>Tennant may also Process images of End User employees, contractors, consumers, or other designated agents taken incidentally by BrainOS-enabled Robots while providing the Services. However, Tennant will not Process any additional identifying information to make any such person identifiable.</p> <p>The Data Subjects are the End User employees, contractors, or other designated agents who have access to the Services.</p> <p>No sensitive data is at issue.</p>
Period of Time Data Will be Retained	The End User Personal Data will be stored for no longer than is necessary or appropriate in light of the purpose of the Agreement and subject to applicable laws, decisions, and guidelines of regulatory authorities.
Sub-processor Transfers	For information on Sub-processor transfers, please refer to Appendix III .

Appendix II – Security Measures

Tennant’s safeguards include appropriate technical, physical, and organizational measures, standards, requirements, specifications, or obligations designed to ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected, taking into account the state of the art; costs of implementation; the nature, scope, context, and purposes of Processing; and the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Appendix III – Approved Sub-processors

Tennant's approved Sub-processors include, without limitation, Brain Corporation, a California corporation.

Appendix IV – Jurisdiction Specific Terms

California:

- (1) The following additional terms apply related to the Processing of End User Personal Data of California residents:
 - a. Each of the Parties will comply with the California Consumer Privacy Act (“CCPA”), as amended by the California Privacy Rights Act (“CPRA”) (collectively, “**California Privacy Law**”)
 - b. To the extent that Tennant collects any End User Personal Data (for purposes of this Appendix, Personal Data as defined under California Privacy Law) of any “consumer” (as defined under California Privacy Law) for Processing (as defined under California Privacy Law) on behalf of the End User pursuant to the Agreement, Tennant shall:
 - i. be a “Service Provider” to the End User under the California Privacy Law;
 - ii. not “sell” or “share” (as such terms are defined under California Privacy Law) Personal Data;
 - iii. not retain, use or otherwise disclose the Personal Data for any purpose other than for the specific purpose of the Services or as otherwise permitted by the California Privacy Law, including for any “business purpose” (as defined under California Privacy Law);
 - iv. confirm that any authorized subcontractor or third party to whom Service Provider discloses or provides access to Personal Data is subject to substantially similar obligations;
 - v. not retain, use or otherwise disclose the Personal Data outside of the direct relationship between End User and Tennant;
 - vi. not combine Personal Data with other personal data collected by Tennant from sources other than End User;
 - vii. after the completion of Services, Service Provider shall, at End User’s direction, delete all Personal Data Processed on your behalf, or return to you all Personal Data Processed on its behalf and delete existing copies;
 - viii. grant you rights to take reasonable and appropriate steps, to help ensure that Tennant is using the Personal Data transferred in a manner consistent with End User’s obligations under California Privacy Law. Tennant must without undue delay notify End User if it makes a determination that it can no longer comply with the requirements of California Privacy Law; and
 - ix. comply with and provide the same level of privacy protection as is required by California Privacy Laws, to the extent applicable to Tennant’s Processing of the Personal Data..
- (2) If Tennant authorizes any subcontractor to Process Personal Data of the End User, Tennant shall enter into contractual provisions so that such subcontractor, service provider or third party is a “service provider” as defined in the CCPA and not a “third party” as defined under California Privacy Law.

Canada:

- (1) The following additional terms apply related to the Processing of Personal Data of Canadian residents:
 - a. To the extent any Sub-processor Processes End User Personal Data associated with Canadian residents, such Sub-processor is a third party under the Personal Information Protection and Electronic Documents Act, with whom Tennant has entered into a written contract with substantially similar protections as set forth in this Addendum. Further, Tennant conducts appropriate due diligence on any such Sub-processor.

Appendix V Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

Having regard to the European Commission’s implementing decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in Third Countries which do not ensure an adequate level of data protection pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

End User (as defined in the EULA)

The data exporting organization (the “**data exporter**”)

- And –

Tennant Sales and Service Company (or such other affiliate of Tennant Company as may be referred to in the EULA)

(the “**data importer**”)

each a “party”; together “the parties”,

HAVE AGREED on the Standard Contractual Clauses for the transfer of Personal Data to Third Countries from a Controller in the European Economic Area to a Processor in the United States pursuant to the European Commission implementing decision of 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in Third Countries under Regulation (EU) 2016/679 of the European Parliament and of the Council (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the Personal Data specified in Appendix 1.

The Clauses are attached hereto by reference with the options and optional modules selected as follows:

- All Sections: Module TWO
- Section I, Clause 7: the optional docking clause will not apply.
- Section II, Clause 9(a): OPTION 2, general written authorization for sub-processing.
- Section II, Clause 11(a): the optional language shall not apply.
- Section IV, Clause 17: OPTION 1, the location of the data exporter.
- Section IV, Clause 18: the jurisdiction associated with the data exporter.

Annex I, II, III, and IV are attached to the Clauses hereto.

ANNEX I TO APPENDIX V

A. LIST OF PARTIES

Data exporter(s): End User, the Data Controller (as defined in the EULA)

Data importer(s): Tennant Sales and Service Company (or such other affiliate of Tennant Company as may be referred to in the EULA), the Data Processor,

B. DESCRIPTION OF THE TRANSFER

The parties agree that the details of Tennant’s Processing activities are set forth in Appendix I to the Addendum.

ANNEX II TO APPENDIX V

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA.

The parties agree that the technical and organization measures are set forth in Appendix II to the Addendum.

ANNEX III TO APPENDIX V

LIST OF SUB-PROCESSORS

The parties agree that the list of approved Sub-processors is set forth in Appendix III to the Addendum.