Leslie AI LLC — Data Processing Addendum

Version 1.0 · Effective November 1, 2026 · Incorporated into the Agreement by the Order Form

This Data Processing Addendum ("DPA") sets out how Leslie AI processes Personal Data on Customer's behalf. Capitalized terms not defined here have the meanings given in the Master Terms.

1. Definitions

Term	Meaning
Personal Data	Customer Data that identifies or can reasonably be linked to an individual.
Data Protection Laws	U.S. federal and state laws on the privacy and security of Personal Data that apply to a party's processing under the Agreement, including state consumer privacy and data breach notification laws.
Processing	Any operation on Personal Data, such as collecting, storing, using, disclosing or deleting it.
Data Subject	The individual a piece of Personal Data relates to.

2. Roles and Instructions

2.1 Roles. Customer is the business or controller of Personal Data, and Leslie AI is Customer's service provider, contractor or processor. Where Customer processes Personal Data on behalf of a property owner as that owner's processor, Leslie AI is Customer's subprocessor, and this DPA applies the same way.

2.2 Instructions. Leslie AI will process Personal Data only to provide the Services, on Customer's documented instructions. The Agreement and Customer's configuration of the Services are Customer's complete instructions. Leslie AI will tell Customer if it believes an instruction violates Data Protection Laws.

2.3 Customer's Responsibilities. Customer is responsible for the lawfulness of the Personal Data it provides and for giving any notices and obtaining any consents Data Protection Laws require.

3. Scope of Processing

Item	Description
Purpose	Only these business purposes: syncing property, lease, resident and ledger records with Customer's Connected Systems; sending Automated Communications Customer has authorized; recording Ledger Entries within Customer's configured parameters; generating Output for Customer; and supporting, securing, troubleshooting and maintaining the Services
Duration	The term of the Agreement plus the return and deletion periods in Section 9
Data Subjects	Residents, owners, applicants, prospects and vendors of Customer, and Customer's Authorized Users
Categories of Personal Data	Names, contact details, property and lease details, ledger and payment status, communications, maintenance requests, call transcripts, identity verification status and session reference for self-guided showings (no ID images or selfies), and user account data
Excluded data	Social Security numbers, full bank or card numbers, government ID images, selfies or other biometric data, and consumer screening reports. Customer will not send these through the Services, including in messages or attachments, and Leslie AI will delete any it receives incidentally. A Pipeline that needs any of them may be enabled only under a separate signed addendum describing the data flow, each party's responsibilities and retention

4. Restrictions

Leslie AI will not:

- sell or share Personal Data, as those terms are used in state consumer privacy laws;
- retain, use or disclose Personal Data for any purpose other than providing the Services, or outside its direct business relationship with Customer;
- combine Personal Data with data from other sources, except to create Aggregated Statistics or as Data Protection Laws allow; or
- use Personal Data to train or fine-tune any machine-learning model, whether generally available, private or internal, or permit a Subprocessor to do so. Running, monitoring, testing and troubleshooting the Services for Customer is not training, and Aggregated Statistics created under the Master Terms are de-identified and are not Personal Data.

5. Personnel

Leslie AI will limit access to Personal Data to personnel who need it to provide the Services, bind them to confidentiality, and train them on handling it securely.

6. Security

6.1 Safeguards. Leslie AI will maintain administrative, technical and physical safeguards appropriate to the risk, including at least:

- encryption of Personal Data in transit and at rest;
- access controls based on least privilege, with multi-factor authentication for systems holding Personal Data;
- logging and monitoring of access to production systems;
- regular backups and tested recovery;
- vulnerability management and timely patching; and
- security review of Subprocessors before engaging them.

6.2 Security Summary. Leslie AI will maintain a written summary of its security program and provide it to Customer on request, as Leslie AI's Confidential Information.

7. Security Incidents

7.1 Notice. Leslie AI will give Customer an initial notice of a Security Incident without undue delay, and within 72 hours of becoming aware of it or sooner if Data Protection Laws require, with details to follow as they become known. Notices go to Customer's legal notice address or to a security contact Customer names. Leslie AI's security contact is Leslie@LesliePM.com. Leslie AI will require its Subprocessors to notify it of security incidents promptly enough for Leslie AI to meet these deadlines.

7.2 Content. The notice will describe, to the extent known: what happened, the Personal Data and Data Subjects affected, the likely consequences, and the steps Leslie AI has taken or will take. Leslie AI will update Customer as it learns more.

7.3 Help with Notifications. Leslie AI will give Customer reasonable help to meet Customer's own obligations to notify individuals or regulators. Customer decides whether and how to notify them, unless the law requires Leslie AI to notify directly.

8. Subprocessors

8.1 Authorization. Customer authorizes Leslie AI to use the Subprocessors on its published Subprocessor List.

8.2 Changes. Leslie AI will give at least 30 days' notice, by email to Customer's legal notice address and to subscribers of the list, before adding or replacing a Subprocessor that processes Personal Data. Customer may object on reasonable data protection grounds, as set out in Section 7.8 of the Master Terms.

8.3 Flow-Down. Leslie AI will bind each Subprocessor to written data protection terms at least as protective as this DPA, and remains responsible for its Subprocessors' performance.

9. Return and Deletion

9.1 Export. On written request made within 30 days after the Agreement ends, Leslie AI will provide one machine-readable export of Customer Data, including records of Automated Communications, at no charge.

9.2 Deletion. Within 90 days after the 30-day export period ends, Leslie AI will delete Personal Data from its active systems, or return it instead if Customer asks and Data Protection Laws require, unless the law requires Leslie AI to keep some. Copies in

backups are deleted within 30 days after that as backups expire, and stay protected under this DPA until then. Leslie AI will have its Subprocessors delete Personal Data on the same schedule, and will confirm deletion in writing on request.

10. Data Subject Requests

If Leslie AI receives a request from a Data Subject about Customer's Personal Data, it will send the request to Customer and will not respond except as Customer instructs or the law requires. Leslie AI will give Customer reasonable help to respond to any request Data Subjects make under Data Protection Laws, including to access, correct, delete or port Personal Data or to opt out of its processing, and reasonable help with data protection assessments and regulator inquiries about the Services.

11. Audits

11.1 Information. Once a year, on request, Leslie AI will provide its security summary and reasonable answers to Customer's security questionnaire.

11.2 Audits. Document review under Section 11.1 comes first. If it does not reasonably show Leslie AI's compliance with this DPA, after a Security Incident, or where Data Protection Laws or a regulator require it, Customer or an independent auditor bound by confidentiality may audit that compliance. Audits will be on 30 days' notice unless law or urgent circumstances require less, during business hours, no more than once a year except after a Security Incident or as law requires, and at Customer's cost unless the audit finds a material breach or law requires otherwise.

12. Specific Laws

12.1 State Privacy Laws. Where a state consumer privacy law applies, Leslie AI will meet the obligations that law places on service providers or processors and certifies that it understands the restrictions in Section 4. Leslie AI will notify Customer if it determines it can no longer meet those obligations. Customer may take reasonable steps to stop and remediate unauthorized use of Personal Data, including suspending the affected processing.

12.2 Gramm-Leach-Bliley Act. If Customer is a financial institution subject to the FTC Safeguards Rule, the parties may sign a separate rider describing the safeguards Leslie AI supports for that rule. Without a signed rider, Leslie AI makes no Safeguards Rule

commitment beyond this DPA.

13. Order of Precedence

If this DPA conflicts with the Master Terms on the processing of Personal Data, this DPA controls. This matches Section 1.2 of the Master Terms. A breach of this DPA is a breach of Section 7.7 of the Master Terms, and liability for it is subject to the enhanced cap in Section 10.3 of the Master Terms.