HOUSBE, L.L.C. — Data Processing Addendum (DPA)

Version 1.0

Effective Date: [Provided on the registration page]

1. Parties; Roles; Incorporation

This DPA forms part of the applicable agreement between HOUSBE, L.L.C. ("HOUSBE") and the customer entity ("Customer"). When processing Customer Personal Data on behalf of Customer, HOUSBE acts as a Processor (and as a Service Provider/Contractor under CCPA/CPRA). For HOUSBE's own operational data (e.g., billing, platform security, service improvement), HOUSBE acts as an independent Controller. Capitalized terms not defined herein have the meanings in the Agreement.

2. Scope; Processing Instructions

HOUSBE will process Customer Personal Data solely on documented instructions from Customer, including with respect to the subject matter, nature and purpose of processing, the types of personal data and categories of data subjects, the duration, and the locations of processing as described in Annex I. Customer is responsible for obtaining all necessary notices and consents.

3. CCPA/CPRA Service Provider & Contractor Terms

No Sale/Share: HOUSBE does not sell or share Customer Personal Data.

Restricted Use: HOUSBE will not retain, use, or disclose Customer Personal Data for any purpose other than the business purposes specified in the Agreement and this DPA, including not for cross-context behavioral advertising.

No Combination: HOUSBE will not combine Customer Personal Data with personal information that HOUSBE receives from another source, except as permitted by CCPA/CPRA.

Certifications: HOUSBE certifies that it understands and will comply with the restrictions herein.

4. Sub-processors

Customer authorizes HOUSBE to engage sub-processors to support the services, subject to a written agreement imposing data protection obligations no less protective than those set out in this DPA.

HOUSBE will maintain a current list of sub-processors and will provide notice of new sub-processors at least 15 days prior to engagement. Customer may reasonably object to a new sub-processor; if the parties cannot agree on a resolution, Customer may suspend the affected services.

5. Security Measures

HOUSBE will implement and maintain appropriate technical and organizational measures ("TOMs") to protect Customer Personal Data as set forth in Annex II. Measures include access controls, least privilege, encryption in transit, logical separation, logging and monitoring, vulnerability management, secure development practices, backups/BCP/DR, vendor risk management, and incident response.

6. Personal Data Breach Notification

HOUSBE will notify Customer without undue delay and, where legally required, within 72 hours after becoming aware of a Personal Data Breach affecting Customer Personal Data. Such notice will describe the nature of the breach, the categories and approximate number of data subjects concerned, the likely consequences, and measures taken or proposed to address the breach.

7. Assistance

Taking into account the nature of processing, HOUSBE will assist Customer, at Customer's request, in fulfilling obligations to respond to data subject requests (access, correction, deletion, portability), conduct data protection impact assessments (DPIAs), and consult with supervisory authorities where required.

8. Government Requests

If HOUSBE receives a legally binding request from a public authority for Customer Personal Data, HOUSBE will (i) notify Customer, unless prohibited by law; (ii) assess the legality of the request; and (iii) disclose only the minimum data necessary to comply.

9. International Transfers

Where HOUSBE transfers Customer Personal Data internationally, HOUSBE will ensure appropriate safeguards are in place, such as the EU Standard Contractual Clauses (SCCs) and the UK International Data Transfer Addendum. HOUSBE will conduct and document Transfer Impact Assessments (TIAs/DTIAs) where required.

10. Return and Deletion

Upon termination or expiry of the services, upon Customer request, HOUSBE will return Customer Personal Data and delete remaining copies within 30-60 days, subject to any legal obligations to retain certain data. Backups will be purged in line with standard rotation schedules. HOUSBE will certify deletion upon request.

11. Audits and Reports

Upon reasonable request, HOUSBE will make available information necessary to demonstrate compliance with this DPA, including third-party audit reports (e.g., SOC 2/ISO). If such reports are insufficient, Customer may conduct an on-site audit no more than annually, with reasonable notice, during normal business hours, without disrupting operations, and subject to confidentiality and reimbursement of HOUSBE’s reasonable costs.

12. Liability; Order of Precedence; Governing Law

This DPA prevails over conflicting terms of the Agreement, and any applicable Addenda published by HOUSBE, L.L.C., to the extent of the conflict with respect to data protection. Liability is subject to the limitations and exclusions set forth in the Agreement, except that no party excludes liability that cannot be limited under applicable law. This DPA is governed by the governing law specified in the Agreement; for the EU SCCs, the governing law is that of an EU Member State that recognizes third-party beneficiary rights.

Annex I — Details of Processing

Subject Matter: Provision of the HOUSBE platform and related services.

Duration: For the term of the Agreement + deletion period as specified in Section 10.

Nature and Purpose: Hosting, storage, transmission, lead routing, communications, analytics, security, and support.

Categories of Data Subjects: Platform users (agents, HIAA members, buyers, renters, FSBO sellers, lenders) and prospective clients (leads).

Types of Personal Data: Identifiers, contact details, account data, usage logs, geolocation (approximate), professional/licensing data, payment/billing metadata (tokenized), and communications metadata. No special categories are intentionally required; any such data is discouraged unless strictly necessary.

Annex II — Technical & Organizational Measures (TOMs)

Access Control & Authentication: unique accounts, MFA for privileged access, least privilege, periodic access reviews.

Encryption: TLS in transit; industry-standard encryption for data at rest where applicable; key management processes.

Network Security: segmentation, firewalls, secure configuration baselines, anti-DDoS measures as applicable.

Logging & Monitoring: centralized logs, security event monitoring, anomaly detection, incident response runbooks.

Vulnerability & Patch Management: routine scanning, patch SLAs, penetration testing, secure SDLC, code review.

Data Minimization & Retention: collection limited to necessity; retention schedules; de-identification where feasible.

Backup, Business Continuity & Disaster Recovery: regular backups, tested restore procedures, BCP/DR plans.

Vendor & Sub-processor Risk Management: security and privacy reviews, contractual flow-down obligations, continuous monitoring.

Personnel Security & Training: confidentiality agreements, role-based training, need-to-know access.

Physical Security: data center protections provided by reputable hosting providers (badging, CCTV, visitor controls).

Change Management: documented change control, testing, rollback procedures.

Secure Development: secrets management, dependency scanning, CI/CD controls, environment separation.

Annex III — Authorized Sub-processors

We maintain a current list of authorized sub-processors in the Customer portal. Examples may include cloud infrastructure, email/SMS delivery, analytics, and customer support tooling. We will notify Customer of additions or replacements at least 15 days before engagement and provide a mechanism to object.