

Privacy Policy

UBoss LLC

A Delaware Limited Liability Company

Effective Date: May 1, 2025

Last Updated: May 1, 2025

Section 1. Introduction and Scope

This Privacy Policy (“Policy”) describes how **UBoss LLC** (“UBoss,” “Company,” “we,” “us,” or “our”), a limited liability company organized under the laws of the State of Delaware and physically operating in the Commonwealth of Massachusetts, collects, uses, stores, shares, and protects information obtained through our websites, platforms, automation services, and related tools.

This Policy applies to:

- Our primary website at **UBoss.ai**;
- Our automation platform hosted at **uboss.work**;
- All forms, integrations, and automation workflows operated or maintained by UBoss on behalf of ourselves or our clients (“Tenants”);
- Any communications initiated through our systems, including but not limited to SMS, WhatsApp, email, and voice calls facilitated via third-party services such as Twilio.

By submitting information through any UBoss-operated form, platform, or communication channel, you (“User,” “you,” or “your”) acknowledge that you have read, understood, and agree to the terms of this Policy. If you do not agree, you must discontinue use of our services and contact us to request removal of any previously submitted data.

UBoss reserves the right to amend this Policy at any time. Material changes will be posted on our website(s) and, where practicable, communicated to affected parties. Continued use of our services following any amendment constitutes acceptance of the revised Policy.

Section 2. Definitions

For the purposes of this Policy, the following terms shall have the meanings set forth below:

Data Controller

The entity that determines the purposes and means of processing personal data. UBoss acts as a Data Controller when collecting information directly from Users for its own business purposes.

Data Processor

The entity that processes personal data on behalf of a Data Controller. UBoss acts as a Data Processor when executing automation workflows on behalf of a Tenant.

Tenant

A business client of UBoss that engages our services to build and operate automation workflows. Tenants may have their own end-users or customers (“Third-Party End-Users”).

Third-Party End-User

An individual who interacts with an automation workflow built by UBoss on behalf of a Tenant. Third-Party End-Users are customers or contacts of the Tenant, not of UBoss directly.

Personal Data / Personally Identifiable Information (PII)

Any information that can be used to identify, contact, or locate an individual, including but not limited to full name, mailing address, telephone number, email address, and preferred communication channel.

Sensitive Data

A subset of Personal Data that includes Social Security numbers, financial account information, health insurance data, government-issued identification numbers, and any data classified as sensitive under applicable federal or state law. *UBoss does not currently collect Sensitive Data; however, this Policy contemplates future scenarios in which such collection may become necessary in connection with expanded service offerings.*

Subprocessor

A third-party service provider engaged by UBoss to assist in the processing or storage of data (e.g., Tally.so, Twilio, Stripe).

Transactional Communication

A non-promotional message sent to a User or Third-Party End-User for the purpose of confirming a form submission, providing a status update, or facilitating a service-related notification.

Section 3. Information We Collect**3.1. Information Currently Collected**

As of the effective date of this Policy, UBoss collects the following categories of Personal Data:

- Full legal name
- Mailing address
- Telephone number(s)
- Email address(es)
- Preferred communication channel (e.g., SMS, email, WhatsApp, phone call)

This information is collected primarily through online forms hosted by Tally.so, a third-party form provider, and is transmitted to UBoss systems via webhook or API integration.

3.2. Information That May Be Collected in the Future

UBoss anticipates that future service offerings may require the collection of additional data categories, which may include but are not limited to:

- Social Security numbers
- Bank account or financial institution information
- Health insurance or healthcare-related data
- Government-issued identification numbers
- Payment card information (processed via Stripe or a comparable PCI-DSS compliant payment processor)

Important: Should UBoss begin collecting any category of Sensitive Data, the following conditions will apply:

1. Affected Users will be notified and asked to provide explicit, informed consent prior to collection;
2. Additional technical and administrative safeguards will be implemented in accordance with applicable law and industry standards;
3. This Policy will be updated to reflect the specific categories of Sensitive Data collected, the purposes for collection, and the retention schedule applicable thereto.

The existence of data fields within our systems capable of storing Sensitive Data does not constitute collection of such data. Collection occurs only when data is actively submitted by a User or provided by a Tenant and processed by UBoss systems.

Section 4. How We Collect Information

UBoss collects information through the following methods:

1. **Online Forms (Tally.so):** Users submit information through forms hosted on the Tally.so platform. Tally.so is a third-party service and maintains its own privacy policy governing data processed on its infrastructure. UBoss receives submitted data via automated webhook or API transmission. By completing and submitting a Tally.so form linked to UBoss services, the User consents to the transfer and processing of their data by UBoss.
2. **Direct Communication:** Users or Tenants may provide information directly to UBoss via email, telephone, messaging platforms, or in-person consultation.
3. **Tenant-Provided Data:** Tenants may supply data regarding their Third-Party End-Users for the purpose of configuring and operating automation workflows. In such cases, the Tenant represents and warrants that they have obtained all necessary consents from their Third-Party End-Users prior to sharing such data with UBoss.
4. **Future Collection Methods:** UBoss may implement additional collection methods in the future, including but not limited to website analytics, account registration portals, payment processing integrations, and cloud-hosted application interfaces. This Policy will be updated accordingly.

Section 5. Third-Party Subprocessors

UBoss engages the following third-party services (“Subprocessors”) in the course of providing its services. Each Subprocessor maintains its own privacy policy and terms of service:

1. **Tally.so** — Online form hosting and data collection. Data submitted through Tally.so forms is transmitted to UBoss systems. Tally.so may process and temporarily store form submissions on its own infrastructure.
2. **Twilio** — SMS, WhatsApp, and voice communication services. UBoss uses Twilio to send Transactional Communications on behalf of itself and its Tenants. All messaging conducted through Twilio is subject to Twilio’s Acceptable Use Policy, the Telephone Consumer Protection Act (TCPA), and applicable FCC regulations including 10DLC registration requirements.
3. **Vercel / GitHub Pages** — Website hosting for UBoss.ai. These platforms may collect standard web server logs (IP address, browser type, access timestamps).
4. **Stripe (Future)** — Payment processing. If and when UBoss implements online payment functionality, payment card data will be processed exclusively by Stripe in accordance with

PCI-DSS standards. UBoss will not store, process, or have access to full payment card numbers.

5. **Anthropic** (*Conditional Fallback*) — AI language model provider. In rare cases where UBoss's self-hosted AI infrastructure is insufficient, requests may be routed to Anthropic's API. Data transmitted is limited to the minimum necessary for the task and does not include raw personally identifiable information. Anthropic's privacy policy and data processing terms govern data processed on their infrastructure.
6. **OpenAI** (*Conditional Fallback*) — AI language model provider. Used as an alternative fallback under the same conditions and restrictions as Anthropic above. OpenAI's privacy policy and data processing terms apply.
7. **Amazon Web Services (AWS)** (*Future*) — Cloud infrastructure. If and when UBoss migrates to cloud-hosted infrastructure, appropriate network security controls, encryption, and access management will be implemented.

UBoss may engage additional Subprocessors as business needs evolve. Material additions to this list will be reflected in updates to this Policy.

UBoss exercises commercially reasonable diligence in selecting Subprocessors but **does not guarantee and shall not be held liable for** the privacy practices, security measures, or data handling of any third-party Subprocessor. Users are encouraged to review the privacy policies of each Subprocessor independently.

Section 6. Purpose and Legal Basis for Processing

UBoss processes Personal Data for the following purposes:

1. **Service Delivery:** To provide, configure, and operate automation workflows for Tenants and their Third-Party End-Users.
2. **Transactional Communications:** To send non-promotional notifications including form submission confirmations, job status updates, appointment confirmations, and service-related alerts.
3. **Client Relationship Management:** To maintain records of business relationships, respond to inquiries, and provide customer support.
4. **Compliance and Legal Obligations:** To comply with applicable federal, state, and local laws, including data breach notification requirements under Massachusetts General Laws Chapter 93H.
5. **Security and Fraud Prevention:** To protect UBoss systems, detect unauthorized access, and maintain the integrity of our infrastructure.
6. **Business Operations:** To manage invoicing, contracts, and internal business processes.
7. **Analytics and Service Improvement:** To create anonymized, de-identified, and aggregated datasets for use in improving UBoss tools, training machine learning models, generating industry benchmarks, and developing commercial analytics insights. Such datasets will not contain personally identifiable information and will not be more granular than zip code or city-level geography.

Legal Basis: Processing is conducted on the basis of (a) the User's consent as expressed through form submission or direct communication; (b) the performance of a contract between UBoss and a Tenant; (c) compliance with legal obligations; and (d) UBoss's legitimate business interests, provided such interests do not override the rights of the data subject.

Section 7. Consent and Opt-In

7.1. Form-Based Consent

All Tally.so forms operated by or on behalf of UBoss include a clear and conspicuous disclosure stating that submission of the form constitutes consent to the collection and processing of the submitted data by UBoss LLC for the purposes described in this Policy. Users who do not wish to consent should not submit the form.

7.2. Messaging Consent (TCPA / 10DLC Compliance)

By providing a telephone number and indicating SMS or WhatsApp as a preferred or acceptable communication channel, the User expressly consents to receive Transactional Communications from UBoss via Twilio-powered messaging services. This consent is subject to the following conditions:

- **No Promotional Messaging:** UBoss does not send promotional, marketing, or advertising messages via SMS, WhatsApp, or voice. All messaging is strictly transactional in nature. Any promotional or advertising outreach will be conducted independently through appropriate channels (e.g., social media platforms) and in compliance with those platforms' policies and applicable law.
- **10DLC Registration:** UBoss maintains appropriate 10DLC campaign registration with applicable carriers and The Campaign Registry (TCR) as required for A2P (Application-to-Person) messaging.
- **Message Frequency:** Message frequency varies based on the nature of the automation workflow. Users will not receive messages unrelated to services they have engaged with.
- **Message and Data Rates:** Standard message and data rates may apply depending on the User's wireless carrier and plan.

7.3. Tenant Responsibility for Third-Party End-User Consent

When UBoss operates automation workflows that involve Third-Party End-Users, the Tenant is responsible for:

1. Obtaining all necessary consents from Third-Party End-Users prior to providing their data to UBoss;
2. Ensuring that appropriate disclosures are made to Third-Party End-Users regarding the nature, purpose, and frequency of any communications;
3. Providing Third-Party End-Users with copies of or access to applicable consent forms, privacy notices, or terms of service;
4. Maintaining records of consent sufficient to demonstrate compliance with TCPA, state law, and Twilio's Acceptable Use Policy.

UBoss will provide Tenants with template disclosure language and consent forms where applicable, but the **Tenant bears ultimate responsibility** for ensuring valid consent has been obtained from their Third-Party End-Users. UBoss shall not be held liable for a Tenant's failure to obtain proper consent.

Section 8. Messaging and Communications

8.1. Channels

UBoss may communicate with Users and Third-Party End-Users through the following channels:

- **SMS / MMS:** Via Twilio, sent from UBoss-registered numbers.
- **WhatsApp:** Via Twilio's WhatsApp Business API, sent from UBoss-registered accounts.
- **Email:** Sent from UBoss-controlled email addresses *or*, in certain automation workflows, from a Tenant's own email account as configured by the Tenant. When email is sent from a Tenant's account, the Tenant is the sender of record and is independently responsible for compliance with the CAN-SPAM Act and applicable state law.

8.2. Nature of Communications

All communications initiated through UBoss automation systems are **transactional in nature** and limited to:

- Confirmation that a form has been submitted or received;
- Updates on the status of a labor job, service request, or project;
- Appointment or scheduling confirmations;
- Requests for additional information necessary to complete a service;
- System or account-related notifications.

UBoss **does not** use its automation systems to send promotional content, advertisements, solicitations, or marketing messages. Any promotional outreach conducted by UBoss or its Tenants will be performed through separate, dedicated channels with independent compliance controls.

Section 9. Opt-Out and Unsubscribe (Off-Ramps)

UBoss respects every individual's right to cease receiving communications. The following opt-out mechanisms are available:

9.1. SMS / WhatsApp

Users and Third-Party End-Users may reply **STOP** to any message received from a UBoss-registered number to immediately cease SMS or WhatsApp communications from that specific number or campaign. Upon receipt of a STOP request, UBoss will:

1. Acknowledge the opt-out with a single confirmation message;
2. Suppress the requesting number from future messaging within the applicable automation workflow;
3. Process the opt-out within a commercially reasonable timeframe, not to exceed ten (10) business days.

9.2. Email

All emails sent through UBoss automation include a functional unsubscribe mechanism in compliance with the CAN-SPAM Act. Emails sent from a Tenant's own email account are subject to the Tenant's own unsubscribe process.

9.3. Multi-Service Opt-Out

UBoss operates multiple automation workflows across multiple communication channels and service categories. Because a single User or Third-Party End-User may be enrolled in more than one workflow:

- An opt-out request applies only to the **specific workflow, channel, or campaign** from which the request originated, unless the User explicitly requests a complete opt-out from all UBoss communications.
- **It is the responsibility of the User or Third-Party End-User to identify which specific service(s) or communication source(s) they wish to discontinue.** UBoss will make commercially reasonable efforts to assist in identifying active workflows, but cannot guarantee identification of all touchpoints without the User's cooperation.
- To request a complete opt-out from all UBoss-operated communications, Users may contact us directly at the contact information provided in Section ??.

9.4. Right to Terminate

UBoss reserves the unilateral right to terminate any automation workflow, communication channel, or data processing activity at any time, for any reason, including but not limited to suspected misuse, legal compliance concerns, or Tenant breach of contract. Exercise of this right shall not constitute a breach of any agreement between UBoss and a Tenant.

Section 10. Multi-Tenant (B2B2C) Responsibilities

UBoss provides automation services to business clients (Tenants) who may, in turn, use those services to interact with their own customers (Third-Party End-Users). This creates a multi-tenant architecture in which responsibilities are allocated as follows:

10.1. UBoss Responsibilities

- Build, configure, and maintain automation workflows to Tenant specifications;
- Implement commercially reasonable security controls aligned with SOC 2 principles;
- Process data in accordance with this Policy and applicable law;
- Provide opt-out and off-ramp mechanisms for communications sent through UBoss-controlled channels;
- Notify Tenants and affected parties in the event of a data breach as required by law;
- Retain the right to terminate or suspend any workflow that UBoss believes, in its sole discretion, violates applicable law, Twilio's Acceptable Use Policy, or this Policy.

10.2. Tenant Responsibilities

Tenants engaging UBoss services represent, warrant, and agree that they shall:

- Obtain and maintain all necessary consents from Third-Party End-Users before providing their data to UBoss or directing UBoss to initiate communications on their behalf;
- Provide Third-Party End-Users with adequate notice regarding the types of communications they will receive and the identity of the parties involved;

- Comply with all applicable federal, state, and local laws governing data privacy, consumer protection, and electronic communications, including but not limited to TCPA, CAN-SPAM, and Massachusetts General Laws Chapters 93A and 93H;
- Refrain from using UBoss automation services to send unsolicited commercial messages, spam, or any communication that violates Twilio’s Acceptable Use Policy;
- Indemnify and hold harmless UBoss from any claims, damages, fines, penalties, or liabilities arising from the Tenant’s failure to comply with the obligations set forth in this section;
- Promptly notify UBoss of any opt-out requests, complaints, or legal actions received from Third-Party End-Users relating to communications sent through UBoss systems.

10.3. Data Ownership

Data collected through UBoss-operated forms and automation workflows is stored in UBoss-controlled databases. Tenants may request export or transfer of data pertaining to their Third-Party End-Users, subject to the following conditions:

- The request must be submitted in writing;
- UBoss will provide the data in a commonly used, machine-readable format within a commercially reasonable timeframe;
- UBoss retains the right to maintain archival copies of data as required for legal compliance, audit, or dispute resolution purposes;
- Upon termination of the Tenant relationship, data will be retained for a period not to exceed ninety (90) days unless a longer retention period is required by law, after which it will be securely deleted.

Section 11. Data Storage and Security

11.1. Current Infrastructure

As of the effective date of this Policy, all data processed by UBoss automation workflows is stored on a **locally owned and operated server** maintained by UBoss LLC. This server runs containerized applications (Docker) hosting the n8n automation platform and associated databases. The server is located in Massachusetts and is under the physical and administrative control of UBoss.

11.2. Security Practices

UBoss implements security practices aligned with the principles of SOC 2 (Service Organization Control 2), including but not limited to:

- Access controls and authentication mechanisms;
- Encryption of data in transit (TLS/SSL);
- Regular software updates and patch management;
- Network segmentation and firewall configuration;
- Logging and monitoring of system access;
- Principle of least privilege for administrative access.

Disclaimer: UBoss has not undergone a formal SOC 2 Type I or Type II audit as of the effective date of this Policy. References to SOC 2 alignment indicate that UBoss voluntarily follows security practices modeled on the SOC 2 Trust Services Criteria. UBoss does not represent or warrant that its security controls have been independently verified or certified.

11.3. Future Infrastructure

UBoss anticipates transitioning certain services to cloud-hosted infrastructure (e.g., Amazon Web Services) in the future. Such migration will include implementation of:

- Virtual Private Cloud (VPC) network isolation;
- Encryption of data at rest and in transit;
- Identity and Access Management (IAM) controls;
- Automated backup and disaster recovery procedures.

This Policy will be updated to reflect infrastructure changes as they are implemented.

Section 12. Data Retention and Deletion

UBoss retains Personal Data only for as long as necessary to fulfill the purposes described in this Policy or as required by applicable law. Specific retention guidelines are as follows:

- **Active Client Data:** Retained for the duration of the business relationship plus ninety (90) days following termination.
- **Archived / Inactive Data:** May be retained in anonymized or aggregated form for analytics and business improvement purposes.
- **Legal Hold:** Data subject to a legal hold, regulatory investigation, or pending litigation will be retained until the matter is resolved, notwithstanding any other retention schedule.
- **Opt-Out Records:** Records of opt-out and unsubscribe requests will be retained indefinitely to ensure continued compliance with suppression obligations.

Deletion Requests: Users may request deletion of their Personal Data by contacting UBoss at the information provided in Section ???. UBoss will process deletion requests within thirty (30) calendar days, subject to any legal retention obligations. Deletion of data from third-party Subprocessor systems is governed by the respective Subprocessor’s data retention policies.

Section 13. Massachusetts State Law Compliance

UBoss operates in the Commonwealth of Massachusetts and complies with applicable Massachusetts data privacy and consumer protection laws, including:

13.1. 201 CMR 17.00 — Standards for the Protection of Personal Information

To the extent that UBoss collects, stores, or processes “personal information” as defined under 201 CMR 17.00 (a Massachusetts resident’s first and last name in combination with a Social Security number, driver’s license number, state ID number, or financial account number), UBoss shall develop and maintain a Written Information Security Program (WISP) that includes administrative, technical, and physical safeguards appropriate to the size, scope, and nature of UBoss’s business.

As of the effective date of this Policy, UBoss does not collect data elements that trigger the WISP requirement under 201 CMR 17.00. Should UBoss begin collecting such data, a WISP will be developed and implemented prior to or concurrent with such collection.

13.2. Massachusetts General Laws Chapter 93A — Consumer Protection

UBoss conducts its business in compliance with Chapter 93A, which prohibits unfair or deceptive acts or practices in trade or commerce. UBoss commits to transparent data practices, honest disclosures, and fair dealing with all Users, Tenants, and Third-Party End-Users.

13.3. Massachusetts General Laws Chapter 93H — Data Breach Notification

In the event of a breach of security involving Personal Data of a Massachusetts resident, UBoss will:

1. Notify the Massachusetts Attorney General’s Office and the Office of Consumer Affairs and Business Regulation as soon as practicable and without unreasonable delay;
2. Notify affected individuals in writing, providing a description of the breach, the types of data involved, and steps the individual may take to protect themselves;
3. Cooperate with law enforcement and regulatory authorities as required;
4. If applicable, notify affected Tenants so they may fulfill their own notification obligations to Third-Party End-Users.

Section 14. Limitation of Liability and Business Protections

14.1. Disclaimer of Warranties

UBOSS PROVIDES ITS SERVICES ON AN “AS IS” AND “AS AVAILABLE” BASIS. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, UBOSS DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. UBOSS DOES NOT WARRANT THAT ITS SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE.

14.2. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL UBOSS, ITS MEMBERS, MANAGERS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF PROFITS, DATA, BUSINESS OPPORTUNITIES, OR GOODWILL, ARISING OUT OF OR IN CONNECTION WITH THIS POLICY, THE SERVICES PROVIDED BY UBOSS, OR ANY DATA BREACH OR UNAUTHORIZED ACCESS, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE) AND EVEN IF UBOSS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

UBOSS’S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS POLICY OR THE SERVICES SHALL NOT EXCEED THE TOTAL FEES PAID BY THE AFFECTED TENANT OR USER TO UBOSS DURING THE TWELVE (12) MONTHS PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

14.3. Indemnification

Each Tenant agrees to indemnify, defend, and hold harmless UBoss LLC, its members, managers, officers, employees, and agents from and against any and all claims, demands, actions, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to:

1. The Tenant's failure to obtain proper consent from Third-Party End-Users;
2. The Tenant's misuse of UBoss automation services;
3. The Tenant's violation of any applicable law, regulation, or third-party terms of service;
4. Any claim by a Third-Party End-User arising from the Tenant's use of UBoss services;
5. The Tenant's provision of inaccurate, misleading, or unlawfully obtained data to UBoss.

14.4. Force Majeure

UBoss shall not be liable for any failure or delay in performance resulting from causes beyond its reasonable control, including but not limited to acts of God, natural disasters, pandemic, government actions, power outages, internet service disruptions, cyberattacks by third parties, or failures of third-party Subprocessors.

14.5. No Third-Party Beneficiaries

This Policy is between UBoss and the User or Tenant. Nothing in this Policy shall be construed to create any rights, obligations, or causes of action in favor of any third party, including Third-Party End-Users, except as expressly set forth herein or as required by applicable law.

Section 15. Children's Privacy

UBoss services are intended for use by businesses and individuals aged eighteen (18) years or older. UBoss does not knowingly collect Personal Data from children under the age of thirteen (13) in compliance with the Children's Online Privacy Protection Act (COPPA). If UBoss becomes aware that it has inadvertently collected data from a child under 13, UBoss will take prompt steps to delete such data and terminate any associated account or workflow.

If you believe that a child under 13 has provided Personal Data to UBoss, please contact us immediately at the information provided in Section ??.

Section 16. Governing Law and Jurisdiction

16.1. Corporate Matters

UBoss LLC is organized under the laws of the **State of Delaware**. Any disputes relating to the formation, governance, or internal affairs of UBoss LLC shall be governed by Delaware law.

16.2. Data Privacy and Consumer Protection

All matters relating to data privacy, consumer protection, electronic communications, and the processing of Personal Data shall be governed by the laws of the **Commonwealth of Massachusetts**, without regard to its conflict-of-law principles, to the extent that the User or data subject is a Massachusetts resident or the data was collected in connection with UBoss's Massachusetts operations.

16.3. Federal Law

This Policy is subject to applicable federal laws, including but not limited to the Telephone Consumer Protection Act (TCPA), the CAN-SPAM Act, the Children’s Online Privacy Protection Act (COPPA), and regulations promulgated by the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC).

16.4. Dispute Resolution

Any dispute arising out of or relating to this Policy shall first be subject to good-faith negotiation between the parties for a period of thirty (30) days. If the dispute cannot be resolved through negotiation, it shall be submitted to binding arbitration in accordance with the rules of the American Arbitration Association (AAA), with the arbitration to be conducted in Massachusetts. Each party shall bear its own costs and attorneys’ fees, unless the arbitrator determines otherwise.

Section 17. Changes to This Policy

UBoss reserves the right to modify, amend, or replace this Policy at any time. When changes are made:

- The “Last Updated” date at the top of this document will be revised;
- Material changes will be posted prominently on UBoss.ai;
- Where feasible, Tenants with active service agreements will be notified via email or other reasonable means;
- Continued use of UBoss services after the posting of changes constitutes acceptance of the revised Policy.

UBoss encourages all Users and Tenants to review this Policy periodically.

Section 18. Contact Information

For questions, concerns, data access requests, deletion requests, or opt-out requests, please contact:

UBoss LLC

Privacy and Data Protection Inquiries

Email: support@uboss.ai

Website: <https://uboss.ai>

Mailing address available upon request.

*End of Privacy Policy — UBoss LLC
Effective May 1, 2025*