

HOA PORTAL PRIVACY POLICY

I. INTRODUCTION AND SCOPE

Summary

This Privacy Policy explains how Oktriva Ventures LLC d/b/a OKTRIVA AI SOLUTIONS ("Company," "we," "us," or "our") collects, uses, processes, stores, shares, protects, and retains information in connection with the HOA Portal, Resident Portal, administrative dashboard, mobile applications, websites, communications, and related services (collectively, the "Services"). This Section explains the purpose of this Privacy Policy, identifies the Company, defines its scope, and describes its relationship to other governing documents.

1.1 Purpose of this Privacy Policy

The purpose of this Privacy Policy is to provide transparency regarding the Company's information-handling practices and to explain how information may be collected, used, processed, stored, disclosed, retained, and protected in connection with the Services.

This Privacy Policy is intended to help Residents, homeowners, tenants, board members, committee members, Administrators, HOA Clients, and other authorized users understand how information is handled when interacting with the HOA Portal and related Services.

The Company is committed to handling information in a manner consistent with applicable laws, reasonable business practices, operational requirements, and the legitimate needs of the Services.

1.2 Company Identification

This Privacy Policy is provided by Oktriva Ventures LLC d/b/a OKTRIVA AI SOLUTIONS.

The Company provides technology services, software solutions, digital platforms, automation tools, communication systems, resident-access tools, and related technology services designed to support homeowners' associations and community-management operations.

For purposes of this Privacy Policy, references to "Company," "we," "us," or "our" refer to Oktriva Ventures LLC d/b/a OKTRIVA AI SOLUTIONS and its authorized service providers, contractors, affiliates, and representatives acting on its behalf in connection with the Services.

The Company acts as a technology service provider and platform operator. The Company is not the homeowner's association, property manager, board of directors, financial administrator, election administrator, or governing authority responsible for community operations.

1.3 Scope of Application

This Privacy Policy applies to information collected, processed, maintained, transmitted, stored, disclosed, or otherwise handled through:

- (a) the HOA Portal and Resident Portal;
- (b) administrator dashboards and management interfaces;
- (c) user accounts and registration processes;
- (d) community communication tools and messaging features;
- (e) voting-related and participation-related features;
- (f) dues-related and account-information features;

- (g) forms, inquiries, support requests, and communications;
- (h) websites, applications, and digital platforms operated by the Company in connection with the Services; and
- (i) other interactions between users and the Company relating to the Services.

This Privacy Policy applies to Residents, homeowners, tenants, HOA Clients, Administrators, board members, committee members, authorized users, visitors, and other individuals whose information may be processed through the Services.

1.4 Relationship to Other Documents

This Privacy Policy forms part of the overall legal framework governing the Services and should be read together with the HOA Portal Master Terms of Service, HOA Portal Cookie Policy, HOA Portal Service Agreement, and any other applicable agreements, disclosures, notices, or policies.

Additional terms, obligations, disclosures, or requirements may apply depending on the specific Services being used, the relationship between the Company and the applicable HOA Client, and the features enabled within the Portal.

In the event a privacy-related matter is specifically addressed in this Privacy Policy, this Privacy Policy shall govern that matter. For operational, service-related, liability, acceptable-use, governance, or contractual matters, users should also review the applicable governing documents referenced above.

Nothing in this Privacy Policy alters the responsibilities of an HOA Client regarding HOA governance, resident management, elections, financial administration, community operations, or compliance with applicable laws and governing documents.

2. INFORMATION WE COLLECT

Summary

This Section describes the categories of information that may be collected through the HOA Portal and related Services. Information may be provided directly by users, supplied by HOA Clients or Administrators, collected automatically through technology systems, obtained from Third-Party Services, or generated through user interactions with Portal features.

2.1 Information You Provide Directly

The Company may collect information that users voluntarily provide when registering for accounts, accessing the Portal, completing forms, communicating through the Services, submitting requests, updating account information, participating in community activities, or otherwise interacting with the Portal.

Such information may include:

- (a) name;
- (b) email address;
- (c) phone number;
- (d) mailing address;
- (e) property address;

- (f) unit number or lot number;
- (g) account credentials;
- (h) communication preferences;
- (i) uploaded documents or files;
- (j) support requests;
- (k) messages, inquiries, comments, or submissions; and
- (l) other information voluntarily provided by the user.

Users are responsible for ensuring that information submitted through the Portal is accurate, complete, and current.

2.2 Resident Information

The Company may collect, receive, process, store, or display Resident Information supplied by HOA Clients, Administrators, Residents, or other authorized individuals.

Resident Information may include information relating to homeowners, tenants, occupants, residents, board members, committee members, and other authorized users.

Such information may include:

- (a) names and contact information;
- (b) property addresses and community-related information;
- (c) resident account information;
- (d) residency or occupancy information;
- (e) role assignments and permissions;
- (f) communication records;
- (g) dues-related information;
- (h) voting-related information;
- (i) maintenance requests or submissions; and
- (j) other HOA-related information maintained through the Portal.

The categories of Resident Information collected may vary depending on the HOA Client's configuration, operational requirements, and enabled Portal features.

2.3 HOA Client and Administrator Information

The Company may collect information relating to HOA Clients, Administrators, board members, committee members, property managers, management companies, and other authorized representatives.

Such information may include:

- (a) business and organizational information;
- (b) administrator account information;

- (c) user-access permissions;
- (d) contact information;
- (e) service-related communications;
- (f) account-management information;
- (g) billing and subscription information;
- (h) support and implementation information; and
- (i) information necessary to provide, maintain, administer, and support the Services.

This information helps the Company manage client relationships, administer Portal functionality, and provide support services.

2.4 Information Collected Automatically

When users access or interact with the Portal, certain technical and usage information may be collected automatically through cookies, authentication systems, security tools, analytics technologies, server logs, and related technologies.

Such information may include:

- (a) IP addresses;
- (b) browser type and version;
- (c) device identifiers;
- (d) operating system information;
- (e) access dates and times;
- (f) pages viewed and features accessed;
- (g) login activity;
- (h) usage patterns and interactions;
- (i) diagnostic information; and
- (j) security-related information.

Automatically collected information helps support Portal functionality, security, performance monitoring, troubleshooting, analytics, and service improvement.

2.5 Information from Third Parties

The Company may receive information from Third-Party Services, integrations, service providers, authentication providers, payment processors, cloud-service providers, communication platforms, analytics providers, AI providers, and other external sources used in connection with the Services.

Information received from third parties may include:

- (a) account-verification information;
- (b) authentication and login information;
- (c) payment-related information;

- (d) service-integration data;
- (e) communication-related information;
- (f) analytics information;
- (g) technical information; and
- (h) other information necessary to support Portal functionality.

The information received depends on the third-party services utilized by the HOA Client and the features enabled within the Portal.

2.6 Voting, Communication, and Portal Activity Information

The Company may collect information relating to user participation in Portal activities and community-management functions.

Such information may include:

- (a) voting participation records;
- (b) survey responses;
- (c) ballot submissions;
- (d) communication activity;
- (e) messages and inquiries;
- (f) announcement interactions;
- (g) document-access activity;
- (h) resident requests and submissions;
- (i) account activity logs; and
- (j) other interactions with Portal features.

This information may be used to operate, administer, secure, support, and improve the Services and to facilitate the functionality requested by HOA Clients and authorized users.

The Company does not use voting-related information to make governance decisions, determine election outcomes, or administer elections on behalf of HOA Clients.

3. HOW WE USE INFORMATION

Summary

This Section explains the purposes for which the Company may use information collected through the HOA Portal and related Services. Information is used to operate, maintain, secure, improve, and support the Services, facilitate HOA-related functionality, communicate with users, and comply with legal and operational obligations.

3.1 Portal Operations and Account Management

The Company may use information to provide, operate, maintain, administer, and support the HOA Portal and related Services.

Such uses may include:

- (a) creating and managing user accounts;
- (b) authenticating users and controlling access permissions;
- (c) providing Portal functionality and features;
- (d) administering resident and administrator access;
- (e) processing requests and submissions;
- (f) maintaining records and account information;
- (g) providing customer support and technical assistance; and
- (h) performing other activities necessary for the operation of the Services.

The Company uses information to ensure that users can access and utilize the Portal in accordance with applicable permissions and system requirements.

The Company may access, review, process, store, transmit, and otherwise handle Resident Information, HOA Data, communications, documents, records, and account information solely as reasonably necessary to provide, operate, maintain, secure, troubleshoot, support, improve, and administer the Services, comply with legal obligations, and fulfill its contractual responsibilities. The Company does not use such information for unrelated personal purposes, unauthorized marketing, resale, or other purposes outside the scope of providing the Services, except as authorized by the applicable HOA Client or required by law.

3.2 Communications and Notifications

The Company may use information to facilitate communications between the Company, HOA Clients, Administrators, Residents, and other authorized users.

Such communications may include:

- (a) account-related notices;
- (b) authentication and security notifications;
- (c) support communications;
- (d) service announcements;
- (e) maintenance notices;
- (f) Portal alerts and reminders;
- (g) community-related communications facilitated through the Portal; and
- (h) other operational communications relating to the Services.

The Company may also use contact information to respond to inquiries, requests, support issues, and other communications submitted through the Portal.

3.3 HOA Administration Support

The Company may use information to support the administrative functionality requested by HOA Clients and authorized users.

Such activities may include:

- (a) resident account administration;
- (b) document management and distribution;
- (c) community communication tools;
- (d) dues-visibility functionality;
- (e) workflow management;
- (f) role-based access administration;
- (g) records organization; and
- (h) other HOA-related operational features supported by the Portal.

The Company uses information solely to facilitate the operation of the technology platform and does not assume responsibility for HOA governance, elections, financial administration, or community decision-making.

3.4 Voting and Community Participation Features

Where voting-related, survey-related, polling, feedback, or community participation features are enabled, the Company may use information to facilitate the technical operation of such functionality.

Such uses may include:

- (a) processing ballot submissions;
- (b) recording participation activity;
- (c) maintaining voting-related records;
- (d) facilitating surveys and community feedback tools;
- (e) supporting election-related workflows; and
- (f) providing reporting and administrative functionality requested by HOA Clients.

The Company does not use voting-related information to determine voting eligibility, certify election results, administer elections, or make governance decisions on behalf of HOA Clients.

3.5 Security and Fraud Prevention

The Company may use information to help protect the security, integrity, availability, and reliability of the Services.

Such activities may include:

- (a) account authentication;
- (b) monitoring access activity;
- (c) detecting unauthorized access attempts;

- (d) investigating security incidents;
- (e) preventing fraud, abuse, or misuse of the Portal;
- (f) enforcing security controls;
- (g) protecting Resident Information and HOA Content; and
- (h) maintaining the overall security of the Services.

The Company may use technical, usage, and security-related information to identify and respond to threats, vulnerabilities, and operational risks.

3.6 Analytics and Service Improvement

The Company may use information to evaluate, analyze, improve, maintain, enhance, and develop the Services.

Such activities may include:

- (a) monitoring system performance;
- (b) evaluating feature usage;
- (c) troubleshooting technical issues;
- (d) improving user experience;
- (e) analyzing usage trends and operational metrics;
- (f) enhancing security and reliability;
- (g) developing new features and functionality; and
- (h) supporting business operations and service improvements.

Information used for analytics may be aggregated, de-identified, or otherwise processed in a manner designed to support operational and business purposes.

3.7 Legal and Compliance Purposes

The Company may use information where reasonably necessary to comply with applicable laws, regulations, legal obligations, contractual requirements, governmental requests, court orders, legal processes, or regulatory requirements.

Such uses may include:

- (a) responding to lawful requests and investigations;
- (b) enforcing legal rights and contractual obligations;
- (c) protecting the Company, HOA Clients, users, and third parties;
- (d) maintaining records required by law;
- (e) resolving disputes and complaints;
- (f) supporting audits, investigations, and compliance activities; and
- (g) complying with applicable legal and regulatory requirements.

The Company may also use information where reasonably necessary to establish, exercise, or defend legal claims and to protect the security, integrity, and lawful operation of the Services.

4. HOW WE SHARE INFORMATION

Summary

This Section explains the circumstances under which information may be shared with HOA Clients, Administrators, service providers, third-party technology providers, legal authorities, and other parties in connection with the operation of the HOA Portal and related Services.

4.1 Sharing with HOA Clients and Administrators

The Company may share information with the applicable HOA Client, Administrators, board members, committee members, property managers, management companies, and other authorized representatives as necessary to operate and administer the Portal.

Such sharing may include:

- (a) Resident Information;
- (b) account information;
- (c) communication records;
- (d) voting-related information;
- (e) dues-related information;
- (f) support requests and submissions;
- (g) activity records; and
- (h) other information maintained through the Portal.

The extent of information shared may depend upon user roles, permissions, HOA requirements, and administrative settings established by the HOA Client.

The HOA Client remains responsible for determining who is authorized to access information through the Portal.

4.2 Service Providers and Vendors

The Company may share information with trusted service providers, contractors, vendors, consultants, and technology partners that assist in providing, operating, maintaining, securing, supporting, or improving the Services.

Such providers may include:

- (a) hosting providers;
- (b) cloud-service providers;
- (c) infrastructure providers;
- (d) authentication providers;
- (e) communication-service providers;

- (f) analytics providers;
- (g) customer-support providers;
- (h) security-service providers; and
- (i) other operational service providers.

These parties may access information only as reasonably necessary to perform services on behalf of the Company and subject to applicable contractual, confidentiality, security, and legal obligations.

4.3 Third-Party Integrations

The Portal may integrate with Third-Party Services, platforms, applications, payment providers, accounting systems, AI technologies, communication tools, and other external systems selected by the Company or an HOA Client. Where such integrations are utilized, information may be shared with the applicable third-party provider to facilitate functionality, interoperability, user requests, or operational requirements.

The type of information shared depends upon the integration involved, the services enabled, and the actions taken by users or HOA Clients. Third-Party Services operate independently from the Company and may be governed by separate privacy policies, terms of service, and data-handling practices.

4.4 Legal Requirements and Protection of Rights

The Company may disclose information where reasonably necessary to:

- (a) comply with applicable laws, regulations, legal processes, subpoenas, court orders, or governmental requests;
- (b) enforce these Terms, contractual obligations, or applicable policies;
- (c) investigate suspected fraud, security incidents, unlawful activity, or misuse of the Services;
- (d) protect the rights, property, safety, security, or interests of the Company, HOA Clients, users, residents, or third parties;
- (e) establish, exercise, or defend legal claims; or
- (f) satisfy other legal, regulatory, compliance, or enforcement obligations.

The Company may also disclose information when it reasonably believes such disclosure is necessary to prevent harm, address security concerns, or protect the integrity of the Services.

4.5 Business Transfers and Corporate Transactions

Information may be disclosed, transferred, assigned, or otherwise made available in connection with a proposed or completed merger, acquisition, financing transaction, reorganization, restructuring, sale of assets, business transfer, investment transaction, bankruptcy proceeding, or similar corporate event involving the Company. In such circumstances, information may be shared with prospective or actual purchasers, investors, lenders, advisors, auditors, legal counsel, consultants, and other parties involved in evaluating or completing the transaction.

The Company may take reasonable measures to ensure that information remains subject to appropriate confidentiality and security protections during such transactions.

4.6 User-Directed Sharing

The Portal may include features that allow users to voluntarily share information, documents, messages, requests, submissions, voting-related information, community content, or other materials with HOA Clients, Administrators, Residents, Authorized Users, or other permitted recipients.

Information shared through such features may be visible to recipients selected by the user or authorized through applicable Portal permissions.

Users are responsible for evaluating the information they choose to share and understanding the audience that may have access to such information through the Portal.

The Company is not responsible for how recipients use, retain, distribute, disclose, or otherwise handle information that users voluntarily choose to share through Portal functionality.

5. THIRD-PARTY SERVICES AND AI TECHNOLOGIES

Summary

This Section explains the Company's use of third-party service providers, hosting and infrastructure providers, AI and automation technologies, payment-related service providers, and other external technologies that may support the operation of the HOA Portal and related Services.

5.1 Third-Party Service Providers

The Company may utilize Third-Party Services, vendors, contractors, consultants, and technology providers to support the operation, maintenance, security, administration, enhancement, and delivery of the Services.

Such providers may assist with:

- (a) hosting and infrastructure services;
- (b) authentication and account management;
- (c) communications and notifications;
- (d) customer support;
- (e) security monitoring and protection;
- (f) analytics and performance monitoring;
- (g) software development and maintenance;
- (h) data storage and backup services; and
- (i) other operational and business functions.

The Company may provide such providers with access to information as reasonably necessary to perform services on the Company's behalf and subject to appropriate contractual, confidentiality, security, and legal obligations.

5.2 Hosting, Cloud, and Infrastructure Providers

The Company may use third-party hosting providers, cloud-service providers, infrastructure vendors, database providers, content-delivery providers, storage providers, authentication services, and related technology partners to support the Services.

These providers may process, store, transmit, secure, back up, or otherwise handle information necessary for the operation of the Portal.

Information maintained through the Portal may be stored on systems operated by third-party infrastructure providers located within the United States or other jurisdictions where such providers maintain facilities.

The Company selects service providers based on operational, technical, security, and business considerations but does not own or directly control the independent operations of such providers.

5.3 AI and Automation Technologies

The Services may incorporate artificial intelligence technologies, machine-learning tools, automation platforms, intelligent workflows, digital assistants, content-generation tools, analytics technologies, and other automated systems.

These technologies may be used to support activities such as:

- (a) workflow automation;
- (b) communication assistance;
- (c) content organization;
- (d) administrative support functions;
- (e) reporting and analytics;
- (f) data processing;
- (g) resident-support features; and
- (h) other operational functions within the Portal.

Certain AI-enabled functionality may be provided through Third-Party Services and external technology providers.

Information processed through AI-enabled features may be transmitted to, processed by, or stored by authorized technology providers to facilitate the requested functionality.

The Company does not guarantee the accuracy, completeness, reliability, or suitability of AI-generated outputs and encourages appropriate human review of automated results.

5.4 Payment and Financial Service Providers

The Portal may integrate with or provide access to third-party payment processors, financial technology providers, accounting platforms, invoicing systems, billing services, banking integrations, or related financial-service providers.

Where such services are utilized, information necessary to facilitate payment-related functionality may be shared with the applicable provider.

The Company does not operate as a financial institution, payment processor, bank, collection agency, accounting firm, or financial administrator.

Payment-related information may be collected, processed, stored, and managed by independent third-party providers in accordance with their own terms, privacy practices, and operational procedures.

Users should review the applicable policies of any payment-related provider before utilizing such services.

5.5 Third-Party Privacy Practices

Third-Party Services, technology providers, integrations, websites, applications, platforms, and external services may maintain privacy practices that differ from those of the Company.

The Company does not control and is not responsible for the privacy policies, data-handling practices, security measures, operational procedures, or business practices of independent third parties.

When users interact with Third-Party Services through or in connection with the Portal, information may be subject to the privacy policies and practices of the applicable provider.

Users are encouraged to review the privacy policies, terms of service, and related documentation of any Third-Party Services they choose to access or utilize.

The inclusion of a Third-Party Service within or alongside the Portal does not constitute the Company's endorsement of the provider's privacy, security, operational, or business practices.

6. COOKIES AND SIMILAR TECHNOLOGIES

Summary

This Section explains how the Company may use cookies, authentication technologies, analytics tools, and similar technologies in connection with the HOA Portal and related Services. These technologies help support functionality, security, account access, performance monitoring, and user experience.

6.1 Types of Cookies Used

The Company may use cookies and similar technologies to support the operation, security, functionality, administration, and improvement of the Services.

Cookies are small text files stored on a user's device that enable websites and applications to recognize devices, remember preferences, maintain sessions, and support functionality.

The types of cookies that may be used include:

- (a) essential cookies necessary for Portal functionality;
- (b) authentication and security cookies;
- (c) performance and analytics cookies;
- (d) functionality and preference cookies;
- (e) session-management cookies; and
- (f) other technologies reasonably necessary to operate and improve the Services.

Certain cookies may be placed directly by the Company, while others may be provided through authorized Third-Party Services.

6.2 Authentication and Session Technologies

The Company may use authentication technologies, session identifiers, security tokens, access controls, and related technologies to support secure account access and Portal functionality.

These technologies may be used to:

- (a) authenticate users;
- (b) maintain login sessions;
- (c) verify account permissions;
- (d) protect accounts from unauthorized access;
- (e) support security monitoring; and
- (f) facilitate secure use of the Services.

Disabling certain authentication or session technologies may limit the availability or functionality of portions of the Portal.

The Company may also use security-related technologies designed to detect suspicious activity, prevent fraud, and protect Resident Information and Portal resources.

6.3 Analytics Technologies

The Company may use analytics technologies, monitoring tools, diagnostic services, and related technologies to better understand how the Services are used.

These technologies may collect information relating to:

- (a) page views and feature usage;
- (b) user interactions;
- (c) navigation patterns;
- (d) device and browser information;
- (e) performance metrics;
- (f) system diagnostics; and
- (g) other operational information.

Analytics information helps the Company evaluate Portal performance, improve user experience, identify technical issues, enhance security, and develop new features and functionality.

Analytics data may be collected directly by the Company or through authorized Third-Party Services.

6.4 Performance and Functionality Technologies

The Company may use technologies designed to improve Portal performance, reliability, customization, and functionality.

Such technologies may support:

- (a) user preferences and settings;
- (b) language and display preferences;
- (c) feature customization;
- (d) system optimization;
- (e) content delivery;
- (f) service reliability; and
- (g) operational efficiency.

These technologies help provide a more consistent and effective user experience across different devices, browsers, and access environments.

The Company may periodically update, replace, modify, or discontinue such technologies as part of ongoing service improvements.

6.5 Cookie Preferences and Controls

Most web browsers and devices provide settings that allow users to manage cookies and similar technologies.

Depending on the browser, device, or operating system used, users may be able to:

- (a) accept or reject certain cookies;
- (b) delete stored cookies;
- (c) manage cookie preferences;
- (d) limit tracking technologies; or
- (e) configure privacy-related settings.

Users should understand that disabling or restricting cookies, authentication technologies, or related functionality may affect the operation, availability, security, performance, or usability of the Portal.

The Company does not guarantee that all Portal features will function properly if cookies or similar technologies are disabled.

Additional information regarding cookie management may be available through browser providers, device manufacturers, or applicable technology platforms used by the user.

7. DATA SECURITY

Summary

This Section explains the measures the Company takes to help protect information processed through the HOA Portal, the inherent limitations of information security, the responsibilities of users and HOA Clients, and how the Company may respond to security incidents affecting the Services.

7.1 Security Measures

The Company implements commercially reasonable administrative, technical, organizational, and physical safeguards designed to help protect information processed through the Services from unauthorized access, disclosure, alteration, misuse, destruction, or loss.

Such measures may include:

- (a) access controls and permission management;
- (b) authentication and account-security mechanisms;
- (c) encryption technologies where appropriate;
- (d) security monitoring and logging;
- (e) infrastructure and network protections;
- (f) backup and recovery procedures;
- (g) vendor and service-provider management practices; and
- (h) other security measures reasonably designed to support the confidentiality, integrity, and availability of information.

The Company periodically reviews and may update its security practices to address evolving technologies, operational requirements, security risks, and industry standards.

7.2 Security Limitations

While the Company takes reasonable measures to help protect information, no website, software platform, cloud environment, communication network, database, device, or technology system can be guaranteed to be completely secure.

The transmission, storage, and processing of information through internet-connected systems involve inherent risks that may be beyond the Company's reasonable control.

Security incidents may result from factors including:

- (a) cyberattacks;
- (b) unauthorized access attempts;
- (c) malware or ransomware;
- (d) phishing attacks;
- (e) compromised credentials;
- (f) software vulnerabilities;
- (g) human error;
- (h) third-party service-provider incidents; or
- (i) other unforeseen circumstances.

Accordingly, the Company does not guarantee the absolute security of information processed through the Services.

7.3 User Security Responsibilities

Users, HOA Clients, Administrators, and authorized representatives play an important role in protecting information and maintaining the security of the Services.

Users are responsible for:

- (a) maintaining the confidentiality of account credentials;
- (b) using strong and secure passwords;
- (c) protecting devices used to access the Portal;
- (d) limiting access to authorized individuals;
- (e) promptly updating account information when necessary;
- (f) reporting suspected unauthorized access or security concerns; and
- (g) complying with applicable security requirements communicated by the Company.

The Company is not responsible for security incidents resulting from a user's failure to maintain appropriate account, device, or credential security.

HOA Clients remain responsible for managing administrative permissions, user access rights, and internal security practices relating to their use of the Portal.

7.4 Incident Response and Security Events

The Company may investigate, respond to, contain, mitigate, remediate, and recover from suspected or actual security incidents affecting the Services.

Where appropriate, the Company may take actions including:

- (a) restricting account access;
- (b) suspending Portal functionality;
- (c) conducting security investigations;
- (d) implementing corrective measures;
- (e) engaging security specialists or service providers; and
- (f) cooperating with law enforcement, regulators, or other authorized parties.

Where required by applicable law, the Company may provide notifications relating to certain security incidents involving information processed through the Services.

The timing, content, and method of any such notification shall be determined in accordance with applicable legal requirements, operational considerations, and the circumstances of the incident.

Nothing in this Privacy Policy shall be interpreted as creating a guarantee that security incidents will not occur or that all incidents can be detected, prevented, mitigated, or resolved.

8. DATA RETENTION

Summary

This Section explains how long information may be retained in connection with the HOA Portal and related Services, the role of HOA Clients in managing community records, the Company's approach to deletion and disposal, and circumstances in which information may be retained to satisfy legal, operational, or compliance requirements.

8.1 Retention Practices

The Company retains information for as long as reasonably necessary to provide, operate, maintain, support, secure, improve, and administer the Services.

Retention periods may vary depending on the nature of the information, the Services being provided, contractual obligations, operational requirements, legal considerations, security needs, and the instructions of the applicable HOA Client.

Information may be retained for purposes including:

- (a) account administration;
- (b) service delivery;
- (c) security monitoring;
- (d) dispute resolution;
- (e) recordkeeping;
- (f) legal compliance;
- (g) system maintenance; and
- (h) other legitimate business and operational purposes.

The Company may periodically review retained information and retention practices to determine whether continued retention remains necessary.

8.2 HOA-Controlled Records

Many records maintained through the Portal are controlled by the applicable HOA Client and may be retained according to the HOA Client's policies, procedures, governance requirements, legal obligations, and operational needs.

Such records may include:

- (a) resident records;
- (b) community communications;
- (c) voting-related records;
- (d) governing documents;
- (e) dues-related information;
- (f) account records;
- (g) maintenance requests; and
- (h) other HOA-related information.

The Company acts as a technology service provider and does not independently determine retention periods for HOA-controlled records except as necessary to operate the Services, comply with legal obligations, or fulfill contractual requirements.

HOA Clients remain responsible for determining appropriate retention practices for their community records and information.

8.3 Deletion and Disposal

The Company may delete, anonymize, de-identify, archive, or dispose of information when it is no longer reasonably necessary for the purposes for which it was collected, retained, or processed.

Deletion may occur:

- (a) upon account closure;
- (b) upon termination of Services;
- (c) at the request of an HOA Client where appropriate;
- (d) pursuant to applicable retention schedules; or
- (e) in accordance with legal, operational, contractual, or security requirements.

Users should understand that deletion may not occur immediately and that backup systems, archived records, legal obligations, technical limitations, and operational requirements may result in temporary retention of certain information.

The Company may also retain de-identified or aggregated information that cannot reasonably be used to identify a specific individual.

8.4 Legal Retention Requirements

Notwithstanding any other provision of this Privacy Policy, the Company may retain information where reasonably necessary to:

- (a) comply with applicable laws, regulations, legal obligations, or governmental requirements;
- (b) respond to lawful requests, subpoenas, court orders, or legal processes;
- (c) establish, exercise, or defend legal claims;
- (d) investigate security incidents, fraud, misuse, or violations of applicable agreements;
- (e) enforce contractual rights and obligations; or
- (f) satisfy audit, compliance, recordkeeping, or reporting requirements.

Where retention is required for legal, regulatory, security, or compliance purposes, the Company may retain applicable information for the period reasonably necessary to satisfy such obligations.

Upon expiration of the applicable retention period, information may be deleted, anonymized, archived, or otherwise handled in accordance with the Company's retention practices and legal obligations.

9. YOUR PRIVACY RIGHTS AND CHOICES

Summary

This Section explains the privacy-related rights and choices that may be available to users regarding information processed through the HOA Portal and related Services. The availability of certain rights may depend upon applicable laws, the user's relationship to an HOA Client, and the nature of the information involved.

9.1 Access Requests

Subject to applicable law and appropriate verification procedures, individuals may request information regarding certain personal information maintained by the Company in connection with the Services.

Where required by applicable law, eligible individuals may request access to information concerning:

- (a) categories of personal information collected;
- (b) sources of information collected;
- (c) purposes for which information is used;
- (d) categories of parties with whom information may be shared; and
- (e) certain personal information maintained by the Company.

The Company may limit access where permitted or required by applicable law, contractual obligations, security requirements, privacy considerations, or the rights of other individuals.

Certain information maintained solely on behalf of an HOA Client may be subject to the HOA Client's control and procedures.

9.2 Correction Requests

Individuals may request correction of personal information that they believe is inaccurate, incomplete, outdated, or incorrect.

Where appropriate and required by applicable law, the Company may take reasonable steps to correct information maintained by the Company.

In certain circumstances, correction requests may need to be directed to the applicable HOA Client where the information is maintained, controlled, or managed by the HOA Client through the Portal.

The Company may request additional information to verify the request and determine whether a correction is appropriate.

9.3 Deletion Requests

Subject to applicable law, contractual obligations, security requirements, operational needs, and legal retention obligations, individuals may request deletion of certain personal information maintained by the Company.

Deletion requests may be denied or limited where retention is necessary to:

- (a) comply with legal obligations;
- (b) complete transactions or provide Services;

- (c) protect security and integrity of the Services;
- (d) establish, exercise, or defend legal claims;
- (e) investigate fraud, misuse, or security incidents; or
- (f) satisfy other lawful business or operational purposes.

Where information is controlled by an HOA Client, deletion requests may need to be submitted to the applicable HOA Client for review and processing.

Deletion of information may not result in the immediate removal of information from backup systems, archives, logs, or records maintained pursuant to legal or operational requirements.

9.4 Communication Preferences

Users may have the ability to manage certain communication preferences associated with their accounts.

Depending on the Services used, users may be able to:

- (a) update contact information;
- (b) modify notification preferences;
- (c) manage certain communication settings; or
- (d) opt out of non-essential communications where permitted.

Certain operational, administrative, account-related, security-related, legal, or service-related communications may continue to be sent even if a user modifies communication preferences.

The Company may continue to communicate where necessary to provide Services, protect accounts, comply with legal obligations, or support Portal operations.

9.5 Privacy Requests and Verification

To help protect privacy and security, the Company may require individuals submitting privacy-related requests to verify their identity before responding to such requests.

Verification procedures may include confirmation of account ownership, identity verification, authentication measures, confirmation of authority, or other reasonable verification steps.

The Company reserves the right to deny, limit, or defer requests where:

- (a) identity cannot be adequately verified;
- (b) the request is fraudulent, abusive, excessive, or unlawful;
- (c) disclosure would adversely affect the rights of others;
- (d) the request conflicts with legal obligations; or
- (e) applicable law otherwise permits or requires such limitation.

Privacy-related requests may be submitted using the contact information provided in this Privacy Policy.

The Company will process verified requests in accordance with applicable law, contractual obligations, operational requirements, and legitimate security considerations.

10. CHILDREN'S PRIVACY

Summary

This Section explains that the HOA Portal and related Services are not intended for use by children and describes the Company's practices regarding information relating to minors.

10.1 Not Intended for Children

The Services are intended for use by homeowners' associations, residents, homeowners, tenants, board members, Administrators, property managers, and other authorized users involved in community-related activities.

The HOA Portal is not directed to children and is not designed or intended to knowingly collect personal information directly from children under the age of thirteen (13).

The Company does not knowingly solicit, collect, use, process, or disclose personal information from children under the age of thirteen (13) through the Services except where such information may be provided by an HOA Client, parent, legal guardian, or authorized adult in connection with legitimate community-management, residency, occupancy, or household-related records.

Where information relating to minors is maintained through the Portal as part of HOA-managed records, such information is generally controlled by the applicable HOA Client and maintained solely for legitimate operational, administrative, residency, or community-related purposes.

10.2 Removal of Children's Information

If the Company becomes aware that personal information has been collected directly from a child under the age of thirteen (13) in a manner inconsistent with applicable law, the Company may take reasonable steps to investigate the matter and, where appropriate, delete or restrict the information.

Parents, legal guardians, HOA Clients, or authorized representatives who believe that a child may have provided personal information through the Services inappropriately may contact the Company using the contact information provided in this Privacy Policy.

Upon receiving a verified request, the Company may take reasonable steps to review the information, determine the appropriate course of action, and comply with applicable legal requirements.

Nothing in this Section limits the Company's ability to retain information where retention is required by law, necessary to protect legal rights, required for security purposes, or maintained by an HOA Client as part of legitimate HOA records, residency records, or community-administration records.

II. U.S. STATE PRIVACY RIGHTS

Summary

This Section describes privacy rights that may be available to certain individuals under applicable U.S. state privacy laws. The availability of specific rights may depend on a person's state of residence, the nature of the information involved, applicable legal requirements, and the Company's role in processing such information.

11.1 State Privacy Rights

Residents of certain U.S. states may have privacy rights under applicable state privacy laws, subject to statutory exceptions, limitations, and eligibility requirements.

Depending on applicable law, such rights may include:

- (a) the right to request access to certain personal information;
- (b) the right to request correction of inaccurate personal information;
- (c) the right to request deletion of certain personal information;
- (d) the right to obtain information regarding categories of personal information collected, used, disclosed, or shared;
- (e) the right to request information regarding certain data-processing activities; and
- (f) other rights provided under applicable privacy laws.

The availability and scope of these rights may vary based on the individual's state of residence, the Company's legal obligations, and the Company's role as a technology service provider acting on behalf of HOA Clients.

In certain circumstances, requests relating to information controlled by an HOA Client may need to be directed to the applicable HOA Client for review and response.

11.2 Verification of Requests

To protect privacy, security, and the rights of individuals, the Company may require verification of identity before processing privacy-related requests.

Verification procedures may include:

- (a) account authentication;
- (b) confirmation of identity;
- (c) verification of account ownership;
- (d) confirmation of authority to act on behalf of another individual; or
- (e) other reasonable verification measures.

The Company may deny, limit, defer, or request additional information regarding a request where:

- (a) identity cannot be adequately verified;
- (b) the request is fraudulent, excessive, repetitive, or unlawful;
- (c) disclosure could adversely affect the rights of others;
- (d) applicable law permits or requires a limitation; or
- (e) the Company lacks sufficient information to process the request.

The Company reserves the right to take reasonable steps necessary to protect information and comply with applicable legal requirements before responding to any privacy-related request.

11.3 Non-Discrimination

The Company will not unlawfully discriminate against an individual for exercising privacy rights available under applicable law.

Subject to applicable legal requirements, individuals who exercise privacy rights will not be denied access to the Services, charged different prices, provided a different level of service, or otherwise treated differently solely because they submitted a valid privacy-related request.

However, the Company may continue to process information, restrict requests, deny requests, or maintain information where permitted or required by applicable law, contractual obligations, security requirements, operational needs, or legitimate business purposes.

Nothing in this Section limits the Company's ability to take actions that are permitted by applicable law or reasonably necessary to provide, secure, maintain, administer, or improve the Services.

12. INTERNATIONAL VISITORS

Summary

This Section explains how information may be processed when individuals access the HOA Portal and related Services from locations outside the United States. It also describes the potential transfer of information across international borders in connection with the operation of the Services.

12.1 Processing in the United States

The Company is based in the United States, and the Services are operated from the United States.

Information collected through the HOA Portal may be processed, stored, maintained, transmitted, accessed, or otherwise handled within the United States by the Company and its authorized service providers.

By accessing or using the Services, individuals located outside the United States acknowledge that their information may be transferred to, processed in, and stored within the United States, where privacy, data-protection, and information-security laws may differ from those in their country, province, state, or jurisdiction of residence.

The Company takes commercially reasonable measures to protect information processed through the Services; however, information may be subject to the laws and legal processes applicable within the United States.

12.2 International Transfers

In connection with the operation, maintenance, support, security, hosting, storage, analytics, communications, automation, and administration of the Services, information may be transferred to, processed by, or made available to authorized service providers, contractors, affiliates, and technology partners located in the United States or other jurisdictions.

Such transfers may occur where reasonably necessary to provide the Services, support Portal functionality, maintain security, facilitate communications, perform technical operations, or comply with legal and contractual obligations.

Where applicable, the Company may implement reasonable measures designed to help protect information during international transfers and to support compliance with applicable legal requirements.

Individuals who access the Services from outside the United States acknowledge and consent to the transfer, processing, storage, and handling of information as described in this Privacy Policy.

Nothing in this Section shall be interpreted as limiting the Company's ability to utilize authorized service providers, infrastructure providers, cloud-service providers, or other technology partners that support the operation of the Services.

13. CHANGES TO THIS PRIVACY POLICY

Summary

This Section explains the Company's right to update, revise, modify, or replace this Privacy Policy from time to time and describes when such changes become effective and how continued use of the HOA Portal constitutes acceptance of the updated Privacy Policy.

13.1 Right to Update this Privacy Policy

The Company reserves the right to modify, amend, update, supplement, revise, or replace this Privacy Policy at any time and in its sole discretion.

Changes may be made for various reasons, including:

- (a) changes to the Services or Portal functionality;
- (b) operational or business changes;
- (c) updates to applicable laws, regulations, or legal requirements;
- (d) privacy, security, or compliance considerations;
- (e) changes involving Third-Party Services or technology providers; or
- (f) improvements to clarify the Company's privacy practices.

The Company may periodically review this Privacy Policy and make updates as necessary to reflect current practices, legal obligations, and operational requirements.

13.2 Effective Date of Changes

Unless otherwise stated, revisions to this Privacy Policy shall become effective upon posting the updated version within the Portal, on an associated website, or through another reasonable method of communication selected by the Company.

The Company may, but is not obligated to, provide notice of material changes through email, Portal notifications, announcements, account notices, or other communication channels.

The "Effective Date" appearing at the beginning of this Privacy Policy shall indicate the date on which the most recent version became effective.

Users are encouraged to review this Privacy Policy periodically to remain informed about the Company's information-handling practices.

13.3 Continued Use of the Portal

By continuing to access or use the Portal after an updated version of this Privacy Policy becomes effective, users acknowledge and accept the revised Privacy Policy to the extent permitted by applicable law.

If a user does not agree with any modification to this Privacy Policy, the user should discontinue use of the Services and, where applicable, contact the HOA Client or the Company regarding available options.

Continued use of the Portal following the effective date of revised privacy terms constitutes acceptance of the updated Privacy Policy and the Company's information-handling practices as described therein.

Nothing in this Section limits any rights or obligations that accrued prior to the effective date of an updated Privacy Policy.

14. CONTACT INFORMATION

Summary

This Section explains how individuals may contact the Company regarding privacy-related questions, requests, legal matters, compliance concerns, and notices relating to this Privacy Policy and the Services.

14.1 General Privacy Inquiries

Individuals with questions, comments, concerns, or requests regarding this Privacy Policy or the Company's privacy practices may contact the Company using the contact information provided on the HOA Portal, the Company's website, or other authorized communication channels designated by the Company.

The Company will make reasonable efforts to review and respond to privacy-related inquiries in accordance with applicable laws, operational requirements, and available resources.

The Company reserves the right to request additional information where reasonably necessary to understand, evaluate, or respond to an inquiry.

14.2 Privacy Requests

Individuals seeking to exercise applicable privacy rights, including requests relating to access, correction, deletion, or other privacy-related matters, may submit requests using the contact methods designated by the Company.

To protect privacy and security, the Company may require verification of identity, account ownership, authority, or other information before processing a request.

Where information is maintained or controlled by an HOA Client, the Company may direct the requesting individual to the applicable HOA Client or coordinate with the HOA Client as appropriate to address the request.

The Company will process verified requests in accordance with applicable law, contractual obligations, operational requirements, and legitimate security considerations.

14.3 Legal and Compliance Matters

Legal notices, regulatory inquiries, compliance-related communications, subpoenas, governmental requests, law-enforcement inquiries, intellectual-property matters, and other formal legal communications should be directed to the Company's designated legal or compliance contact.

The Company reserves the right to request additional information, documentation, verification, or clarification before responding to legal, regulatory, privacy, security, or compliance-related matters.

Nothing in this Privacy Policy obligates the Company to provide legal advice, waive legal rights, admit liability, or take any particular action in response to a legal or compliance inquiry.

The Company may respond to such matters in a manner consistent with applicable law, contractual obligations, security requirements, privacy obligations, and legitimate business interests.

14.4 Notice Procedures

Unless otherwise required by applicable law, notices relating to this Privacy Policy may be delivered by email, Portal notification, website posting, administrative dashboard notification, recognized courier service, postal mail, or other reasonable communication methods selected by the Company.

Users and HOA Clients are responsible for maintaining accurate contact information and for monitoring communications associated with their accounts and use of the Services.

Notices from individuals to the Company shall be deemed received only when actually received through an authorized communication channel designated by the Company.

Notices from the Company shall be deemed given when transmitted, posted, delivered, or otherwise made available through the applicable communication method, unless otherwise required by applicable law.

The Company reserves the right to utilize alternative communication methods where reasonably necessary to protect the Services, address security concerns, comply with legal obligations, respond to emergencies, or communicate important privacy-related information.