REBEL ALLIANCE EARTH

ADAPT AND THRIVE

rebelalliance.earth

PRIVACY POLICY

Governed by the Digital Fairness Code

Your data is yours. This document explains how we protect it.

Version 1.1 | March 12, 2026

Raindrop, LLC dba RebelAlliance.Earth

151 Calle de San Francisco, San Juan, PR 00901

This document is written at an 8th-grade reading level in compliance with DFC Right #14 (Plain Language Requirement).

TABLE OF CONTENTS

1. Introduction and Our Privacy Philosophy

This Privacy Policy explains how Rebel Alliance Earth ("RAE," "we," "us," or "the Platform"), operated by Raindrop, LLC, handles your information when you use our websites, mobile applications, AI services, marketplace, governance tools, and other platform features (collectively, the "Services"). This Policy supplements our Terms and Conditions and is governed by the Digital Fairness Code ("DFC").

RAE exists to give you control over your digital life, not to harvest it. Unlike conventional privacy policies that describe how a company collects and uses your data, this document describes how RAE is architecturally designed to not access your data — and the limited, specific circumstances where data processing is necessary for operations, safety, security, or legal compliance.

This is not a conventional privacy policy because RAE is not a conventional platform. We do not sell your data. We do not monetize your attention. We do not build behavioral profiles for advertising. We do not share your personal information with advertisers, data brokers, or any third party for commercial purposes. These are not just promises — they are enforced by the Platform's architecture: encrypted sovereign storage, edge-first processing, and independently auditable access logs that you control.

> **DFC Reference:** *Rights #10 (PII Privacy), #14 (Plain Language Requirement), #28 (Privacy Engineering Standard)*
>
> **Regulatory Alignment:** *GDPR (Regulation 2016/679), CCPA/CPRA, Brazil LGPD, UK Data Protection Act 2018, Australia Privacy Act 1988*

1.1 Business Information

Data Controller: Raindrop, LLC dba RebelAlliance.Earth

Address: 151 Calle de San Francisco, San Juan, PR 00901, United States

Privacy Contact: privacy@rebelalliance.earth

Governing Law: Laws of the Commonwealth of Puerto Rico, except where superseded by applicable privacy laws in your jurisdiction.

EU Representative (for GDPR purposes): [To be designated upon EU launch]

UK Representative (for UK GDPR purposes): [To be designated upon UK launch]

1.2 Scope

This Privacy Policy applies to all information collected, processed, or stored through the Services. If you access our Services from a jurisdiction with its own data protection laws, those laws apply in addition to this Policy. Where local law provides stronger protections, the stronger protections apply.

> **DFC Reference:** *Rights #24 (Universal Jurisdiction Framework), #25 (Digital Colonialism Provision)*

2. Data Ownership and Sovereignty

You own everything you create, upload, share, or generate on the Platform. This includes all personally identifiable information (PII), personal history, content, interactions, activity data, your social graph, and all data derived from your use of the Platform. RAE does not own your data.

RAE implements and maintains privacy controls designed to prevent the collection, storage, reading, or accessing of your personal data in any human-readable form, except as strictly necessary for operations, safety, security, or legal compliance. These controls include encrypted sovereign storage, auditable access logs, and independent privacy engineering review. Where architectural implementation is in progress, equivalent protections are maintained through organizational and policy controls until the architectural controls are fully deployed.

DFC Reference: *Rights #02 (Data Portability), #10 (PII Privacy), #13 (Full Deletion on Exit)*

2.1 What RAE Does Not Do

RAE does not sell, license, share, or monetize your personal data under any circumstances. RAE does not use your personal data to train general-purpose AI models shared with other users. RAE does not build behavioral profiles for advertising. RAE does not share your data with advertisers, data brokers, or any third party for commercial purposes. RAE does not retain your data after you leave the Platform (see Section 10).

2.2 Your Sovereign Data

The following categories of data are sovereign — they are yours, stored in your encrypted sovereign storage, and inaccessible to RAE except as described in this Policy:

Personal RAG: Everything your Guide has learned about you — your values, preferences, conversation history, and the knowledge base that shapes your Guide's behavior.

Digital Config: Your AI configuration, portable across all devices and services you own.

Communications: All messages sent via the Platform, end-to-end encrypted via Matrix Protocol.

Social Graph: Your connections, relationships, and community memberships.

Content: All text, images, video, and other content you create or upload.

Activity Data: Your browsing history, interaction patterns, and usage data on the Platform.

Consent Records: Immutable logs of every consent you have granted or revoked, stored in your sovereign encrypted storage.

2.3 Operational Telemetry (Not Sovereign Data)

RAE collects limited operational telemetry necessary to maintain and improve Platform performance. This includes error logs, latency metrics, system health data, and aggregated usage statistics. Operational telemetry is collected separately from sovereign user data, is not linked to your identity, and is not used for advertising, profiling, or any commercial purpose. Operational telemetry is governed by this Privacy Policy but is not stored in your sovereign encrypted storage. For clarity: aggregated, de-identified summaries of activity data (such as total page views or feature usage counts) may be treated as operational telemetry once they can no longer be linked to an individual user.

3. Information We Collect and How We Collect It

RAE collects the minimum information necessary to provide and protect the Services. We are transparent about every category of data we touch.

3.1 Information You Provide Directly

Account Registration: Email address, phone number (for verification), and identity verification information at the applicable KYC level (see Terms Section 3.2).

Onboarding Conversation: During your initial conversation with your Guide, you share values, preferences, and privacy settings. This becomes your Personal RAG and is sovereign data.

Content: Text, images, video, and other content you create, upload, or share on the Platform.

Communications: Messages you send to other users, end-to-end encrypted via Matrix Protocol. RAE does not read the content of encrypted messages.

Marketplace Data: Transaction information, shipping addresses, and payment information (processed by third-party payment processors; RAE does not store full payment credentials).

Support Requests: Information you provide when contacting customer service or filing a dispute.

3.2 Information Collected Automatically

Vigilance Layer Signals: Behavioral signals processed by the Vigilance Layer for safety and wellbeing purposes. For adults, this is default-on with opt-out. For minors, it is mandatory. The Vigilance Layer uses a deviation-first model: it monitors for significant deviations from your established patterns, not your patterns themselves. Per-user signals are used solely for safety and wellbeing, not for advertising, growth optimization, or commercial profiling.

Edge-Processed Data: Where technically and commercially feasible, behavioral analysis is processed on your device. Only anonymized, aggregate signals are transmitted to Platform infrastructure. Where device or network limitations require server-side processing, that processing is constrained to the minimum data necessary, encrypted in transit and at rest, and logged.

Aggregate Interest Signals: The Zeitgeist Engine receives anonymized, aggregate interest signals. No individual attribution ever occurs within this system.

Operational Telemetry: Error logs, latency metrics, system health data, and aggregated usage statistics as described in Section 2.3.

3.3 Information We Do Not Collect

RAE does not collect: keystroke data; clipboard contents; contacts from your device; location data (unless you explicitly share it for a specific feature); biometric data; financial account information (beyond what is processed by third-party payment processors for transactions you initiate); or any data from other applications on your device.

4. How We Use Your Information

RAE uses information only for the purposes described below. We do not use your data for any purpose not listed here.

4.1 Service Provision

To operate, maintain, and deliver the Services: rendering content you have chosen to share, routing encrypted messages, processing marketplace transactions, executing Guide conversations, and enabling governance participation.

4.2 Safety and Wellbeing

To operate the Vigilance Layer: compliance monitoring (detecting illegal activity and rule violations), platform health monitoring (detecting coordinated inauthentic behavior and manipulation), and user wellbeing monitoring (detecting distress patterns and providing care through your Guide). The wellbeing features are supportive tools, not emergency services, and cannot guarantee detection or prevention of harm.

4.3 Security

To protect the Platform and users: detecting and preventing fraud, hacking, spam, and other security threats; enforcing the One Real Person Rule; operating graduated KYC verification; and responding to security incidents.

4.4 Legal Compliance

To comply with applicable laws, regulations, and lawful government requests, as described in Section 7.

4.5 Platform Improvement

To improve the Services using anonymized, aggregate data and operational telemetry. RAE does not use your personal data to train general-purpose AI models shared with other users. Anonymized, aggregate usage patterns may be used to improve platform-wide AI quality, but only after removing all personally identifiable information.

4.6 Communication

To send you notices about your account, changes to the Terms or this Policy (through your Guide and by email), and responses to your support requests. RAE does not send unsolicited marketing communications unless you have opted in.

4.7 Compensation

If you have opted in to data compensation, anonymized aggregate signals derived from your activity may generate commercial value. You are entitled to fair and transparent compensation as set forth in the applicable compensation policy. Your Guide may assist with related interactions.

> ▶ **DFC Reference:** *Right #12 (Right to Compensation)*

5. Legal Bases for Processing

Where the GDPR, UK GDPR, or similar frameworks apply, RAE relies on the following legal bases:

5.1 Consent

You have given explicit, affirmative opt-in consent for the specific processing activity. RAE does not use pre-checked boxes, bundled consents, or dark patterns. Every consent you grant is as easy to revoke as it was to give. Your Guide manages your consent settings and can explain them at any time. Immutable consent logs are stored in your sovereign encrypted storage and auditable by you at any time.

> ▶ **DFC Reference:** *Rights #09 (Right to Opt In), #15 (Dark Pattern Prohibition), #16 (Consent Simplicity Standard)*

5.2 Contractual Necessity

Processing is necessary to perform the Services you have requested under the Terms and Conditions — for example, delivering your Guide conversations, processing marketplace transactions, or routing messages.

5.3 Legitimate Interests

Processing is necessary for our legitimate interests in operating and securing the Platform, provided those interests do not override your data protection rights. RAE's legitimate interests are narrowly defined: platform security, fraud prevention, and operational telemetry. RAE does not rely on legitimate interests for advertising, behavioral profiling, or commercial data use.

5.4 Legal Obligations

Processing is necessary to comply with applicable laws and regulations, including anti-money laundering requirements, tax obligations, and responses to lawful government requests.

5.5 Vital Interests

In rare circumstances, processing may be necessary to protect someone's life — for example, when the Vigilance Layer detects crisis signals that indicate imminent risk of harm.

6. When We Share Your Information

RAE shares your information only in the limited circumstances described below. RAE does not sell your data. RAE does not share your data with advertisers or data brokers.

6.1 At Your Direction

When you post content publicly, send messages, participate in marketplace transactions, or use features that involve sharing information with other users, your information is shared as you have directed. Your Guide helps you understand who can see what before you share.

6.2 Service Providers

RAE uses a limited number of third-party service providers who process data on our behalf: payment processors for marketplace transactions; infrastructure providers for hosting and storage (subject to our encryption and access controls); and identity verification providers for KYC compliance. Service providers are contractually bound to process data only as we instruct, to maintain confidentiality, and to implement appropriate security measures. Service providers do not have access to your sovereign encrypted data.

6.3 Legal Requirements

RAE may disclose information as required by law, court order, or lawful government request. See Section 7 for our detailed commitments on government data requests.

6.4 Safety

In emergencies involving imminent risk to life or safety, RAE may share the minimum information necessary with appropriate authorities (for example, emergency services in response to a crisis signal detected by the Vigilance Layer).

6.5 Business Transactions

In the event of a merger, acquisition, or sale of substantially all assets, your data may be transferred to a successor entity. Any successor must agree to be bound by this Privacy Policy and the DFC commitments, or we will provide you with notice and the opportunity to export your data and delete your account before the transfer occurs. If a successor would materially reduce your privacy rights, RAE will seek your explicit opt-in consent where required by applicable law before completing the transfer.

6.6 What We Never Share

RAE does not share: the content of your end-to-end encrypted communications; your Personal RAG or Guide conversation history; your Digital Config or AI training data; your Vigilance Layer wellbeing signals; or any personal data with advertisers, data brokers, or for commercial profiling purposes.

7. Government Data Requests and Transparency

Government requests for your data are disclosed to you unless a court order expressly prohibits notification. RAE will challenge overbroad or unlawful government requests and will notify you of any disclosure as soon as legally permitted.

In cases involving serious criminal activity and valid legal compulsion from a court of competent jurisdiction, RAE may disclose limited, non-content metadata (such as account creation date, last login IP address, or device identifiers) only after internal legal review and only to the minimum extent required by the specific legal instrument. RAE will not voluntarily provide content data (messages, Personal RAG, Guide conversations, or User Content) to any government without a valid, specific court order.

RAE publishes a transparency report detailing the volume, type, jurisdictional origin, and outcome of government data requests.

> **DFC Reference:** *Right #29 (Government Transparency Mandate)*
>
> **Regulatory Alignment:** *GDPR Articles 6(1)(c), 23; US Stored Communications Act; EU e-Evidence Regulation*

8. International Data Transfers

RAE operates globally. When your data crosses jurisdictional borders, RAE applies reasonable standards that meet or exceed the higher of the origin or destination jurisdiction's requirements. RAE may use compliant data centers and infrastructure in jurisdictions that meet these standards. RAE does not exploit jurisdictional gaps to lower your privacy protections.

For transfers from the EEA, UK, or Switzerland, RAE relies on: EU Standard Contractual Clauses (SCCs) as adopted by the European Commission; UK International Data Transfer Agreements (IDTAs) as adopted by the UK Information Commissioner's Office; and supplementary measures including encryption in transit and at rest, access controls, and the sovereign storage architecture described in Section 2.2.

RAE applies the same privacy standards to every user worldwide. RAE does not apply lesser standards to users in developing nations compared to users in any other jurisdiction.

> **DFC Reference:** *Rights #24 (Universal Jurisdiction Framework), #25 (Digital Colonialism Provision)*
>
> **Regulatory Alignment:** *GDPR Chapter V, UK Data Protection Act 2018 Part 2, APEC Cross-Border Privacy Rules, Brazilian LGPD Chapter V*

9. Data Retention

9.1 General Retention Principles

RAE retains your sovereign data for as long as your account is active. Operational telemetry is retained for the minimum period necessary to serve its purpose (typically no more than 90 days for error logs and system health data, and no more than 12 months for aggregated usage statistics).

9.2 Retention After Account Closure

When you close your account: you may export all your data in machine-readable format within 72 hours of request. Complete data deletion occurs within 30 days, independently auditable. Operational telemetry associated with your account is deleted on the same schedule. Legal hold obligations may require limited retention of specific data categories; if so, you will be notified of the legal basis and expected duration.

9.3 Retention for Legal Compliance

Some data may be retained beyond account closure where required by law (for example, transaction records for tax compliance or data preserved under a legal hold). Such retention is limited to the minimum data and minimum period required by the specific legal obligation. Data retained for legal compliance is not used for any other purpose.

9.4 Consent Record Retention

Immutable consent logs are retained for the duration of your account plus 36 months after account closure (or such longer period as required by applicable law) to support audit and compliance verification. You may request a consent audit summary from your Guide at any time.

DFC Reference: *Rights #06 (Right to Exit), #07 (Right to Be Forgotten), #13 (Full Deletion on Exit)*

Regulatory Alignment: *GDPR Articles 5(1)(e) (Storage Limitation), 17 (Right to Erasure); CCPA §1798.105*

10. Your Privacy Rights

The following rights apply to all RAE users worldwide. Where your local law provides additional rights, those rights also apply.

10.1 Rights Under the Digital Fairness Code

These rights are yours by default and apply globally:

Right to Data Ownership: You own all your data. RAE does not own it. (DFC Right #10, Terms Section 1.1)

Right to Data Portability: Export all your data in standard, machine-readable format at any time. (DFC Right #02, Terms Section 1.4)

Right to Exit: Leave the Platform at any time with your data, social graph, content, and Digital Config intact. (DFC Right #06, Terms Section 1.4)

Right to Be Forgotten: Require complete deletion of all personal data, behavioral profiles, and derived inferences. Deletion is verified and independently auditable. (DFC Right #07, Terms Section 1.5)

Right to Opt In: All data collection requires your affirmative opt-in. No pre-checked boxes. (DFC Right #09, Terms Section 8.2)

Right to Compensation: If your data generates commercial value (only if opted in), you are entitled to fair compensation. (DFC Right #12, Terms Section 1.9)

Right to Algorithmic Transparency: Understand why content is shown to you and how algorithms affect your experience. (DFC Right #01, Terms Section 1.6)

Right to Consent Simplicity: Every permission is as easy to revoke as it is to give. (DFC Right #16, Terms Section 8.2)

Right to Audit: Request a personal privacy audit at any time through your Guide, or commission an independent audit at your own expense. (DFC Right #28, Terms Section 8.6)

10.2 Additional Rights Under the GDPR (EEA/UK Residents)

If you reside in the EEA or UK, you additionally have:

Right of Access: Request copies of your personal data. (GDPR Article 15)

Right to Rectification: Request correction of inaccurate or incomplete data. (GDPR Article 16)

Right to Restrict Processing: Request limits on how we process your data in certain circumstances. (GDPR Article 18)

Right to Object: Object to processing based on legitimate interests or for direct marketing. (GDPR Article 21)

Right to Withdraw Consent: Withdraw consent at any time, as easily as you gave it. (GDPR Article 7(3))

Right Not to Be Subject to Automated Decision-Making: Object to decisions made solely by automated processing that significantly affect you. The AI-Assisted Dispute Resolution system provides human escalation rights consistent with this right. (GDPR Article 22)

To exercise any of these rights, contact privacy@rebelalliance.earth or ask your Guide. RAE will respond within 30 days (or the applicable statutory timeframe in your jurisdiction). EU users may also lodge a complaint with their local data protection authority.

Regulatory Alignment: *GDPR Articles 15–22, UK GDPR*

10.3 Additional Rights Under CCPA/CPRA (California Residents)

If you are a California resident, you additionally have:

Right to Know: Request disclosure of categories and specific pieces of personal information collected, used, or disclosed. (CCPA §1798.100)

Right to Delete: Request deletion of your personal information. (CCPA §1798.105)

Right to Correct: Request correction of inaccurate personal information. (CCPA §1798.106)

Right to Opt Out of Sale/Sharing: RAE does not sell or share your personal information as defined by the CCPA. If this changes, you will have the right to opt out. (CCPA §1798.120)

Right to Non-Discrimination: RAE will not discriminate against you for exercising your privacy rights. (CCPA §1798.125)

To exercise these rights, contact privacy@rebelalliance.earth or ask your Guide. RAE will verify your identity and respond within 45 days.

Regulatory Alignment: *CCPA/CPRA (§1798.100–199)*

10.4 Additional Rights in Other Jurisdictions

RAE respects the privacy rights of users in all jurisdictions, including but not limited to: Brazil (LGPD data subject rights), South Korea (PIPA rights), Japan (APPI rights), India (DPDPA 2023 rights), Australia (Privacy Act rights), and Canada (PIPEDA rights). If your local law provides rights not listed here, contact privacy@rebelalliance.earth and we will comply with applicable requirements.

11. Children's Privacy

RAE applies global standards for minor protection aligned with universally accepted human rights principles, including the UN Convention on the Rights of the Child (UNCRC).

11.1 Age Requirements

Users must meet the minimum age requirement for their jurisdiction (see Terms Section 3.1 for regional minimum ages). RAE does not knowingly collect personal information from anyone under the applicable minimum age without verified parental consent. If we discover that we have inadvertently collected such information, we will delete it immediately.

11.2 Protections for Minors

For users under 18: no behavioral profiling; no targeted advertising; no engagement optimization algorithms. Parental controls are available. The Vigilance Layer applies mandatory wellbeing monitoring to all minor accounts with no opt-out. The legitimate rights of children (including age-appropriate privacy, expression, and access to information) are respected alongside parental authority.

DFC Reference: *Rights #31 (Minor Protection Standard), #39 (Minor Wellbeing Standard)*

Regulatory Alignment: *COPPA, UNCRC, UK Age Appropriate Design Code, EU DSA Article 28, California Age-Appropriate Design Code, Australia Online Safety Act*

12. Security Measures

RAE's privacy architecture is the engineering foundation of the Platform, not a policy bolted on after the fact.

12.1 Encryption

User data is stored in user-controlled encrypted storage. Communications are end-to-end encrypted via Matrix Protocol. Decentralized storage (Filecoin) ensures data sovereignty is not dependent on RAE's continued existence. Data is encrypted in transit (TLS 1.3 or equivalent) and at rest (AES-256 or equivalent).

12.2 Access Controls

RAE employees, contractors, and third parties are prohibited from accessing your end-to-end encrypted communications, viewing your Personal RAG, inspecting your Guide's ethos, or reading the training data or behavioral parameters of your Rebel Agent. Access controls are enforced technically (encryption, key management, access-gated infrastructure) and organizationally (policy, audit, and termination for violations). Where server-side processing is required to deliver the Services you have directed, that processing operates on the minimum data necessary, is logged, and is auditable by you.

12.3 Edge-First Processing

Where technically and commercially feasible, behavioral analysis is processed on your device. Only anonymized, aggregate signals are transmitted to Platform infrastructure. Where device or network limitations require server-side processing (for example, low-end devices with limited compute capacity, or users with intermittent connectivity where real-time on-device analysis is not reliable), that processing is constrained to the minimum data necessary, encrypted, and logged. As device capabilities and Platform infrastructure mature, RAE will progressively expand edge processing coverage.

12.4 Incident Response

In the event of a personal data breach, RAE will notify affected users without undue delay and in any event within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to your rights. Notification will include the nature of the breach, likely consequences, measures taken, and your Guide will personally brief you on any steps you should take.

Regulatory Alignment: *GDPR Articles 25, 32–34; CCPA §1798.150; NIS2 Directive*

12.5 Independent Audits

RAE conducts regular internal and independent privacy audits as required by DFC Right #28 (Privacy Engineering Standard). Summaries of these audits, including any material findings and remediation actions, are published to the community through the Platform's transparency reporting.

13. Cookies and Tracking Technologies

RAE uses cookies and similar technologies only for the following purposes:

Strictly Necessary: Session management, authentication, and security. These cookies are required for the Platform to function and cannot be disabled.

Preference: Remembering your language, accessibility settings, and display preferences. You may disable these through your Guide settings.

RAE does not use: advertising or tracking cookies; third-party analytics cookies (such as Google Analytics); cross-site tracking pixels; or any cookie or technology designed to follow your activity across other websites. RAE does not participate in any cross-site advertising network.

You can configure your browser to refuse cookies or to prompt you before accepting them. Disabling strictly necessary cookies may prevent some Platform features from functioning properly. Your Guide can help you manage cookie settings.

Regulatory Alignment: *EU ePrivacy Directive (2002/58/EC), UK PECR, GDPR Recital 30*

14. AI-Specific Privacy Provisions

RAE's AI services (the Guide, the Rebel Agent, the Zeitgeist Engine) process personal data in ways that require specific privacy disclosure.

14.1 Guide and Personal RAG

Your Guide processes your conversations to learn your values, preferences, and communication style. This processing creates your Personal RAG, which is sovereign data stored in your encrypted storage. RAE does not access the Personal RAG for any purpose other than delivering your Guide conversations as you have directed. The Personal RAG will not be accessed, copied, or seized without your explicit consent or lawful due process with notification.

14.2 Rebel Agent

Your Rebel Agent's training data, values alignment, and behavioral parameters are sovereign data. The Platform may intervene in or override agent behavior for safety, security, or legal compliance, with logging and disclosure as described in Terms Section 1.3.

14.3 Zeitgeist Engine

The Zeitgeist Engine processes only aggregate, anonymous signals. Individual attribution does not occur within this system. The Zeitgeist Engine does not identify, target, or profile individual users.

14.4 AI Training Data

RAE does not use your personal data to train general-purpose AI models shared with other users. Anonymized, aggregate usage patterns may be used to improve platform-wide AI quality, but only after removing all personally identifiable information. You may opt out of aggregate data contribution at any time through your Guide settings. Opting out does not affect your access to any Platform features. Your Guide can walk you through this setting during onboarding or at any time afterward.

DFC Reference: *Rights #05 (Value-Aligned AI Disclosure), #33 (AI Agent Sovereignty), #35 (AI Risk Classification)*

Regulatory Alignment: *EU AI Act Articles 10 (Data and Data Governance), 13–14 (Transparency, Human Oversight)*

14.5 Synthetic Media and Avatar Processing

Your Guide's visual and audio presentation is generated using third-party synthetic media technology (currently D-ID). The face and voice you see and hear are AI-generated. Your Guide's underlying ethos, values, memory, and decisions are processed on RAE's sovereign infrastructure and are never shared with the synthetic media provider beyond what is necessary to render the presentation layer. The synthetic media provider does not receive your Personal RAG, your conversation history, or any PII beyond the rendering request. RAE will notify you if the synthetic media provider changes.

DFC Reference: *Right #05 (Value-Aligned AI Disclosure), #33 (AI Agent Sovereignty)*

Regulatory Alignment: *EU AI Act Article 52 (Transparency for Certain AI Systems), emerging state deepfake disclosure laws*

15. Changes to This Policy

We may update this Privacy Policy as the Platform evolves, as regulations change, and as the community's governance decisions warrant. Changes follow the same tiered process as changes to the Terms and Conditions (see Terms Section 2.2):

Non-material changes: Notice via your Guide and/or email, effective immediately or upon reasonable notice.

Material changes: Clear, plain-language notice at least 14 days before changes take effect (or 30 days where required by applicable law).

Substantive changes to privacy rights: At least 30 days notice (or longer if required by law), subject to community governance review through the Voice system.

We will always maintain a current version of this Policy at rebelalliance.earth/privacy.

15.2 Enterprise Survivability

Nothing in this Privacy Policy shall be interpreted to prevent RAE from taking reasonable action necessary to maintain solvency, operational continuity, or legal compliance. This provision ensures that the Platform can survive and continue to serve its community. It does not authorize RAE to circumvent the foundational privacy rights established by the Digital Fairness Code, which remain the Platform's governing principles in all circumstances.

15.3 Human Review

For any privacy-related decision that results in account suspension, data access restriction, or denial of a privacy rights request, you have the right to request and receive review by a qualified human decision-maker. This right applies in addition to any automated processing or AI-assisted review and is provided at no cost to you.

16. Contact Information

For questions about this Privacy Policy, your privacy rights, or our data practices:

Privacy and Data Requests: privacy@rebelalliance.earth

General Inquiries: admin@rebelalliance.earth

Data Protection Officer: [To be designated]

Raindrop, LLC dba RebelAlliance.Earth

151 Calle de San Francisco, San Juan, PR 00901

EU Representative (for GDPR purposes): [To be designated upon EU launch]
UK Representative (for UK GDPR purposes): [To be designated upon UK launch]

▶️ **Regulatory Alignment:** *GDPR Article 27 (Representative in the EU), UK GDPR Article 27*

Your data is yours. This is not a promise. It is how the Platform is built.