REBEL ALLIANCE EARTH

ADAPT AND THRIVE

rebelalliance.earth

TERMS AND CONDITIONS OF SERVICE

Governed by the Digital Fairness Code

7 Principles. 39 Rights. One Global Standard.

Version 2.7 | 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

Preamble: Our Commitment to You

Welcome to Rebel Alliance Earth (“RAE,” “we,” “us,” or “the Platform”). These Terms and Conditions (“Terms”) are not a document designed to protect us from you. They are a mutual agreement between the Platform and you (“you,” “your,” or “the User”) that spells out your rights, our obligations, and the rules that keep this community safe and sovereign.

RAE is the living embodiment of the Digital Fairness Code (“DFC”) — a globally portable rights framework of 39 codified rights organized under 7 foundational principles. Every clause in these Terms is anchored to the DFC. Where any ambiguity exists, the DFC rights prevail in the user’s favor.

RAE exists to give you control over your digital life, not to harvest it. Your messages are end-to-end encrypted. Your Personal RAG, values alignment, and Digital Config are stored in sovereign encrypted infrastructure that RAE does not access for any purpose beyond delivering the Services you have explicitly directed. We do not read your private content for advertising. We do not use your personal data to train models shared with other users. We do not monetize your information. This is not merely a promise — it is enforced by the Platform’s architecture: encrypted storage, zero-knowledge design principles where technically feasible, and independently auditable access logs that you control.

By accessing or using any RAE website, mobile application, AI service, marketplace, governance tool, or other platform feature (collectively, the “Services”), you agree to these Terms and the supplemental policies referenced within them (Privacy Policy, Acceptable Use Policy, Marketplace Policy, and Community Standards). If you do not agree, you should not use the Services.

While these Terms prioritize your rights under the DFC, the Platform reserves the right to process data and enforce rules as reasonably necessary for operations, safety, security, or legal compliance, without undermining your sovereignty. This operational authority exists to run and protect the Platform — not to circumvent your rights.

> ▶ **DFC Reference:** *Right #14: Plain Language Requirement — These Terms are written in plain language at an 8th-grade reading level. No legal jargon is hidden in fine print.*
>
> ▶ **DFC Reference:** *Right #15: Dark Pattern Prohibition — These Terms contain no manipulative design. Your consent is real consent.*
>
> ▶ **DFC Reference:** *Right #16: Consent Simplicity Standard — Every permission you grant is as easy to revoke as it is to give.*

1. Your Rights on the Platform

The following rights are yours by default. They are not granted to you by RAE — they are inherent. RAE's architecture is built to protect and enforce them. These rights apply equally to every user, everywhere in the world, regardless of jurisdiction.

1.1 Data 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, communications, AI training inputs, Personal RAG, or Digital Config in any human-readable form, except as strictly necessary for operations, safety, security, or legal compliance (for example, rendering a post you chose to share publicly, routing an encrypted message you sent, processing a marketplace transaction, or responding to lawful legal process). 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. RAE does not sell, license, share, or monetize your personal data under any circumstances.

> **DFC Reference:** *Rights #02 (Data Portability), #10 (PII Privacy), #12 (Right to Compensation), #13 (Full Deletion on Exit)*
>
> **Regulatory Alignment:** *GDPR Articles 15–20, CCPA/CPRA §1798.100–145, Brazil LGPD, South Korea PIPA, Japan APPI*

1.2 Identity Sovereignty

Your digital identity belongs to you. RAE verifies your identity but does not own it. Your identity credentials are portable, self-sovereign, and not dependent on the Platform for their existence. Your personal AI configuration ("Digital Config") is your property, portable across all devices and services you own.

> **DFC Reference:** *Rights #26 (Decentralized Identity), #27 (Self-Sovereign Identity Standard), #34 (Digital Config Right)*
>
> **Regulatory Alignment:** *EU eIDAS 2.0 Regulation, Utah SB 275 (Digital Identity Model)*

1.3 AI Agent Sovereignty

Your Rebel agent — your personal AI entity on the Platform — is sovereign. Its training data, values alignment, behavioral parameters, and the Personal RAG (everything you have taught it) will not be accessed, copied, seized, or modified without your explicit consent or lawful due process with notification. Your Guide's ethos is your property. The Values RAG engine that drives your Guide is stored on sovereign infrastructure and is not shared with third parties.

Notwithstanding the above, the Platform may intervene in or override AI agent behavior as reasonably necessary for operations, safety, security, or legal compliance — for example, to prevent an agent from being used to coordinate harm, distribute illegal content, or circumvent safety systems. In the case of systemic threats (mass exploitation of a vulnerability, coordinated abuse across multiple accounts, or platform-wide security incidents), RAE may disable classes of agent behavior globally and implement automated mitigations before individual notification, with logging and disclosure as soon as operationally feasible. All interventions are subject to appeal through the dispute resolution process in Section 15.

> **DFC Reference:** *Rights #33 (AI Agent Sovereignty), #05 (Value-Aligned AI Disclosure), #35 (AI Risk Classification)*
>
> **Regulatory Alignment:** *EU AI Act (Regulation 2024/1689), NIST AI Risk Management Framework, Canada AIDA*

1.4 Right to Exit

You may leave the Platform at any time, for any reason, with your data, social graph, content, and Digital Config intact. RAE will not impose penalties, degraded service, or artificial barriers to departure. Upon exit, you may export all personal data in a standard, machine-readable format within 72 hours of request. Complete data deletion occurs within 30 days, independently auditable.

DFC Reference: *Rights #06 (Right to Exit), #02 (Data Portability), #08 (Right to Portability), #13 (Full Deletion on Exit)*

Regulatory Alignment: *GDPR Article 17 (Right to Erasure), Article 20 (Data Portability), CCPA §1798.105*

1.5 Right to Be Forgotten

You may require complete deletion of all personal data, behavioral profiles, and derived inferences. Deletion is verified, confirmed, and independently auditable. This right survives account termination.

DFC Reference: *Right #07 (Right to Be Forgotten)*

1.6 Algorithmic Transparency

RAE discloses the logic, training data sources, and optimization targets of all algorithms that affect your experience. RAE's algorithms optimize for meaningful engagement, not maximum engagement. You have the right to understand why content is shown to you and to participate in setting content moderation and algorithm rules through the Voice governance system.

DFC Reference: *Rights #01 (Algorithmic Transparency), #32 (Algorithmic Governance Right), #37 (Algorithmic Wellbeing Standard)*

Regulatory Alignment: *EU Digital Services Act (DSA) Articles 27, 40; EU AI Act Transparency Requirements*

1.7 Collective Rights

You may organize collectively to negotiate platform terms, features, and policies, consistent with principles of free speech and the right to assemble as recognized under applicable laws (including U.S. First Amendment principles). You may organize and execute collective migration between platforms without Platform interference. RAE will not algorithmically suppress, shadow-ban, or disadvantage organizing activity, provided such activity does not constitute coordinated inauthentic behavior, harassment, or violation of applicable law. RAE will not retaliate against users who advocate for migration, regulation, or collective action.

DFC Reference: *Rights #03 (Collective Bargaining), #19 (Coordinated Migration), #20 (Platform Neutrality in Organizing), #23 (Anti-Retaliation)*

Regulatory Alignment: *EU Digital Markets Act (DMA) Article 6, US First Amendment Principles*

1.8 Creator Ownership

If you create content on the Platform, you retain full ownership. RAE may not claim any license beyond what is strictly necessary to display your content as you have directed within the Platform. This is a fundamental departure from legacy platform terms.

DFC Reference: *Right #36 (Creator Ownership Standard)*

1.9 Right to Compensation

If your data generates commercial value through anonymized, aggregate signals (only if you have opted in), you are entitled to fair and transparent compensation as set forth in the applicable compensation policy from time to time. Your Guide may assist with related interactions on your behalf.

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

1.10 Equal Global Standards

RAE applies the same standards to every user worldwide. RAE does not apply lesser privacy, safety, or rights standards to users in developing nations compared to users in any other jurisdiction. Where local law requires higher standards, RAE meets them; where local law permits lower standards, RAE does not exploit the gap.

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

Regulatory Alignment: *GDPR Extraterritorial Application (Article 3), African Union Data Policy Framework, ASEAN Framework on Digital Data Governance*

2. Acceptance, Modifications, and Plain Language

2.1 Binding Agreement

By accessing or using the Services, you confirm that you have read, understand, and agree to be bound by these Terms and all supplemental policies. Your Guide will walk you through the key provisions during onboarding in a conversational format — not in a form you are expected to scroll past.

2.2 Modifications to Terms

We may update these Terms as the Platform evolves, as regulations change, and as the community's governance decisions warrant. Changes follow a tiered process based on their impact:

Non-material changes (security updates, bug fixes, minor feature adjustments): We will provide notice via your Guide and/or email. Changes take effect immediately or upon reasonable notice.

Material changes (new features, policy updates that do not reduce your rights): We will provide clear, plain-language notice at least 14 days before changes take effect (or 30 days where required by applicable law), delivered through your Guide and by email.

Substantive changes to user rights: We will provide clear, plain-language notice at least 30 days before changes take effect (or such longer period as required by applicable law). These changes are subject to community governance review through the Voice system. Where urgent safety or legal compliance requires faster implementation, changes may take effect immediately with post-implementation community review and an opportunity for reversal if the community objects within 30 days.

DFC Reference: *Right #16: Consent Simplicity Standard — No asymmetric friction in how changes are communicated.*

2.3 Plain Language Commitment

Every term, policy, and consent form on the Platform is written at or below an 8th-grade reading level. If any provision of these Terms is unclear to you, you may ask your Guide for an explanation in your language and register. RAE will maintain translations in all languages where we have significant user populations.

DFC Reference: *Right #14 (Plain Language Requirement)*

Regulatory Alignment: *EU Consumer Rights Directive (2011/83/EU), FTC Clear and Conspicuous Standard*

3. Eligibility and Age-Specific Protections

3.1 General Eligibility

You must be at least 13 years of age (or the minimum digital consent age in your jurisdiction, whichever is higher) to access or use the Services. RAE enforces the One Real Person Rule: every User account must have exactly one verified human behind it. This is enforced architecturally through a graduated Know Your Customer (KYC) system, not merely by policy.

Regional Minimum Ages

The following minimum ages apply based on your jurisdiction of residence. Where your jurisdiction is not listed, the default minimum age of 13 applies unless local law requires a higher age:

European Union: 16 years in most member states (13 in Belgium, Denmark, Estonia, Finland, Latvia, Portugal, Sweden, and the UK under GDPR Article 8 implementation; 14 in Austria, Bulgaria, Cyprus, Italy, Lithuania, Spain; 15 in Czech Republic, France, Greece, Slovenia; 16 in all others). RAE applies the specific age for your member state.

United Kingdom: 13 years, with enhanced protections under the Age Appropriate Design Code applied to all users under 18.

Australia: 16 years for services subject to the Online Safety Act.

South Korea: 14 years, with parental consent required under 14.

Brazil: Parental consent required for users under 16 (LGPD).

All other jurisdictions: 13 years, or the applicable local minimum, whichever is higher.

Regulatory Alignment: *GDPR Article 8, COPPA, UK Age Appropriate Design Code, Australia Online Safety Act, South Korea PIPA, Brazil LGPD*

3.2 Graduated Verification

RAE uses a five-level verification system that scales identity requirements with the level of authority and access requested:

Level 1: Email verification — basic platform access.

Level 2: Phone verification — Collaboration creation, Marketplace buying.

Level 3: Identity verification — Marketplace selling, Voice actions above local level.

Level 4: Enhanced KYC — high-value transactions, organizational representation.

Level 5: Full AML compliance — financial instruments, large-scale economic actions.

Regulatory Alignment: *FATF Recommendations 10–16, EU 6th Anti-Money Laundering Directive, US Bank Secrecy Act, FinCEN requirements*

3.3 Minor Protection Standards

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), prioritizing the highest protections without endorsing suppressive regimes or adopting the most restrictive interpretations from any single jurisdiction. For users under 18:

No behavioral profiling of minors. No targeted advertising to minors. No engagement optimization algorithms applied to minor accounts. Parental controls are available and clearly communicated, but the legitimate rights of children (including age-appropriate privacy, expression, and access to information) are respected alongside parental authority. Parental or guardian consent is required for users between 13 and the age of majority in their jurisdiction. The Vigilance Layer applies mandatory wellbeing monitoring to minor accounts consistent with DFC Rights #31, #38, and #39, including optional parental notification for distress signals.

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

Regulatory Alignment: *COPPA (US), UN Convention on the Rights of the Child, UK Age Appropriate Design Code (Children's Code), EU Digital Services Act (Article 28), California Age-Appropriate Design Code (AB 2273), Australia Online Safety Act*

3.4 Children's Privacy

RAE does not knowingly collect personal information from anyone under 13 (or the applicable minimum age) without verified parental consent. If we discover that we have inadvertently collected such information, we will delete it immediately. To report a concern, contact us at privacy@rebelalliance.earth.

4. Account Registration, Security, and Your Digital Identity

4.1 Account Creation and Onboarding

Account creation is conducted through a guided conversation with your personal AI Guide. During onboarding, your Guide will help you establish your values, preferences, and privacy settings through natural conversation — not through a traditional form. The conversation becomes the foundation of your Guide's ethos (the Personal RAG for your individual account). Privacy and consent settings are established during this conversation, not in a separate form you are expected to find later.

4.2 Your Digital Identity

Your digital identity on the Platform encompasses your values, history, preferences, knowledge, ethos, social graph, and Digital Config. It is sovereign — it will not be seized, copied, or accessed without your explicit consent or lawful due process with notification to you. You may hold multiple roles simultaneously (Member, Contributor, Artisan, Counselor, Mentor, Representative, Artist), earned through community recognition, not assigned by the Platform.

4.3 Account Security

You agree to keep your login credentials confidential and to notify us immediately of any unauthorized access or security breach. RAE provides a pause/investigate toggle (you or customer service can take your account offline for review) and a kill switch for complete account erasure on your request.

4.4 BFFs — Always There

You may designate up to 5 Best Friends who retain limited communication access even if your account is muted or suspended. This social bond is preserved during compliance actions except where maintaining it would violate applicable law or pose an imminent safety risk.

5. Scope of Services

The RAE Platform operates a 15-system architecture organized across four layers: Engagement, Power, Backend and Safety, and Governance. The Services include, but are not limited to:

5.1 Engagement Layer

Community: Social features with parity to major social platforms (posting, sharing, messaging, media), all sovereign by design.

The Guide: Your personal AI avatar — companion, advisor, executor, researcher, proxy, and Digital Config carrier. The Guide is trained on your values and speaks as you would speak.

The Rebel Agent: Your sovereign AI agent that acts on your behalf on and off the Platform.

Collaborations: Groups, causes, missions, movements — the organizing unit for any shared purpose.

Marketplace: Direct-to-creator commerce with platform fees transparently disclosed on every receipt.

5.2 Power Layer

Zeitgeist Engine: Real-time on-platform and off-platform trend intelligence.

Issues, Voice, and Common Agenda: Fractal socio-political organizing, collective voting (K-dimensional), and bottom-up community priorities.

Fractal Governance: Nested democratic governance from groups of 12, scaling from Family level through Council (global).

Government Engine: Global organizational transparency database and precision legislative targeting.

5.3 Backend and Safety Layer

Privacy Architecture: User-owned encrypted storage, zero platform access to PII except as reasonably necessary for operations, safety, security, or legal compliance, with full data portability.

Security Architecture: No outside agents on platform, graduated KYC, kill switch, One Real Person Rule.

Vigilance Layer: Compliance monitoring, platform health monitoring, and user wellbeing monitoring.

Permission System: Fractal-aware access control with six permission layers (Public, Community, Collaboration, Fractal, Personal, Agent).

6. AI Services, the Guide, and the Rebel Agent

6.1 Nature of AI Services

RAE provides AI-driven services including the Guide (personal AI avatar), the Rebel Agent (sovereign AI agent), the Zeitgeist Engine (trend intelligence), and various AI-assisted platform features. These services are powered by a proprietary Values RAG engine combined with third-party language model processing. The AI exists to represent your values, not the Platform's defaults.

6.2 AI Transparency and Disclosure

RAE discloses the values alignment, training methodology, known biases, and optimization targets of all AI systems that affect your experience. The Guide's architecture consists of: (a) a sovereign backend (PII, memory, logic, ethos) on RAE infrastructure; (b) a Values RAG engine (proprietary IP); (c) third-party language model processing; and (d) avatar presentation layer. You are informed about which components handle which aspects of your interactions. When AI-generated content includes synthetic audio, video, or avatar presentation, including your Guide's voice and face, that content is generated by artificial intelligence and is disclosed as such at the point of interaction. RAE will notify you through your Guide when the underlying AI models powering your experience are materially updated, as outputs may change following such updates. **DFC Reference:** *Rights #05 (Value-Aligned AI Disclosure), #35 (AI Risk Classification)*

Regulatory Alignment: *EU AI Act Articles 13–14 (Transparency), 50 (High-Risk AI Obligations), NIST AI RMF, EU AI Act Article 52 (Synthetic Media Disclosure)*

6.3 AI Configuration Rights

Your AI configuration operates on a risk-tiered system aligned with the EU AI Act classification:

Low social risk: Fully configurable at the personal level (humor, daily schedule, communication style).

Medium social risk: Configurable at local or regional fractal consensus (community resource management, shared bot behavior).

High social risk: Subject to expedited alliance-wide or global consensus via time-bound Voice polls, not exceeding 14 days unless extended by community vote (surveillance features, autonomous decision systems).

Catastrophically harmful: Disallowed regardless of consensus.

Notwithstanding the above, the Platform may intervene in or override configurations as reasonably necessary for operations, safety, security, or legal compliance.

6.4 User Input and AI Processing

When you provide text, data, prompts, or other input to the AI Services, that input is processed to provide and improve your personal AI experience. Your input is part of your Personal RAG and is treated as your sovereign data under Section 1.1. RAE does not use your personal input 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.

6.5 AI Content Disclaimer

AI-generated content is provided as a tool to assist you and may contain errors, omissions, or biases. You remain responsible for any decisions or actions you take based on AI content. AI content is not a substitute for professional advice (medical, legal, financial, or otherwise). RAE is continuously improving AI accuracy and welcomes your feedback.

6.6 Prohibited AI Uses

You agree not to use the AI Services: for any unlawful, discriminatory, or harmful purpose; to create false or misleading information intending to defraud or mislead others; to produce content that is harassing, hateful, or invasive of privacy; to attempt to circumvent safety systems; or to generate content depicting the exploitation of minors.

The Platform may monitor and intervene in AI uses as reasonably necessary for operations, safety, security, or legal compliance, overriding agent sovereignty where required to enforce these prohibitions or to respond to imminent risk. All such interventions are logged and disclosed to the affected user.

6.7 The I-to-We Bridge

Your Guide bridges your personal sovereign agent to the collective. It presents collective action opportunities in the context of your own values and lets you decide. The Guide does not act collectively on your behalf without your explicit direction. This is enforced architecturally, not by policy.

6.8 AI-Generated Recommendations and Promoted Content

The Guide and the Marketplace may surface product recommendations, merchant offers, and content suggestions generated or ranked by AI systems. When a recommendation includes a merchant discount drawn from a promotional budget — whether initiated by the merchant or by Platform AI matching — that

is disclosed on the receipt and in the recommendation interface. AI-generated recommendations are not sold to merchants. Merchants cannot pay to improve their ranking or placement in Guide recommendations. Any sponsored or promoted content surfaced by AI is labeled as such at the point of display.

> ▶ **DFC Reference:** *Rights #01 (Algorithmic Transparency), #30 (Marketplace Transparency Standard)* ◀
> **Regulatory Alignment:** *FTC Guides Concerning Endorsements and Testimonials (16 CFR Part 255), EU AI Act Article 13*

7. The Vigilance Layer: Platform Safety and User Wellbeing

The Vigilance Layer is how RAE keeps the Platform safe while respecting your sovereignty. It is fundamentally different from how other platforms monitor their users. Legacy platforms monitor to protect the platform. RAE's Vigilance Layer exists primarily to protect you.

7.1 Compliance and Legal Monitor

The Platform scans for illegal activity and rule violations at jurisdiction-appropriate standards. Content moderation thresholds are set by community vote at the appropriate fractal level — not unilaterally by the Platform. Violations escalate through a defined process: Note, Warn, Instruct, Counsel, Fine, Mute, Suspend, Ban. Local adjudication comes first; escalation to the next fractal layer occurs only if local resolution fails. You always have the right to appeal to the next fractal layer or to the AI-Assisted Dispute Resolution system described in Section 15.

> ▶ **Regulatory Alignment:** *EU Digital Services Act Articles 14–16 (Content Moderation), 20 (Internal Complaint Handling), 21 (Out-of-Court Dispute Settlement)*

7.2 Platform Health Monitor

The Platform monitors for coordinated inauthentic behavior, bot penetration, manipulation of the voting system, and Marketplace gaming. Integrity reports are published to the community at regular intervals with full transparency.

7.3 User Wellbeing Monitor

This is the feature that distinguishes RAE from every other platform. Behavioral signals are monitored by default as part of the Platform's care architecture, with responses handled primarily by your Guide. This is care, not surveillance, and is powered by AI to minimize intrusion and maximize relevance.

Specifically: excessive usage patterns trigger a Guide check-in; compulsive return patterns are surfaced and discussed privately; isolation signals prompt connection suggestions; language distress signals trigger a caring Guide response with appropriate resources; crisis signals trigger immediate Guide intervention plus crisis resources.

Adult users may adjust monitoring sensitivity or opt out entirely through their Guide settings. Minor accounts are subject to mandatory wellbeing monitoring consistent with DFC Rights #31, #38, and #39, with optional parental notification for distress signals. Minors will not be permitted to opt out of wellbeing monitoring.

The wellbeing features are supportive tools, not emergency services, and cannot guarantee detection or prevention of harm. If you or someone you know is in immediate danger, contact local emergency services.

Design Principle: Deviation-First Monitoring

The Vigilance Layer is designed around a core principle: pattern deviations, not patterns themselves, are the meaningful signal. The Platform does not build comprehensive behavioral profiles of your habitual activity. Instead, AI systems monitor for significant deviations from your established patterns that may indicate distress, crisis, or unhealthy engagement changes. This deviation-first approach minimizes data processing, maximizes relevance, and ensures that the Platform's care architecture engages only when it matters — not continuously.

DFC Reference: *Rights #37 (Algorithmic Wellbeing Standard), #38 (Crisis Response Obligation), #39 (Minor Wellbeing Standard)*

Regulatory Alignment: *EU AI Act (Emotional Recognition Limitations), UK Online Safety Act, US Kids Online Safety Act provisions*

7.4 Data Processing for Safety

The Vigilance Layer and Zeitgeist Engine use different data scopes. The Zeitgeist Engine uses only aggregate, anonymous signals — individual attribution does not occur within this system. Individual votes in the Voice system are private. The Vigilance Layer uses per-user behavioral signals solely for safety and wellbeing purposes, not for advertising, growth optimization, or commercial profiling. All processing is logged and auditable by you at any time. RAE has engaged certified privacy engineers and submits to independent audits as required by DFC Right #28.

Design Principle: The Algorithm Goes to You

RAE's privacy architecture is built on a foundational design choice: where technically and commercially feasible, the algorithm moves to your device — your data does not move to a central server. Behavioral pattern analysis, deviation detection, and Guide interactions are processed as close to you as possible, with only anonymized, aggregate signals ever 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. This edge-first processing principle minimizes the data RAE ever touches, structurally limits what any breach or government request could expose, and ensures that the most sensitive processing — your values, your patterns, your Guide's understanding of you — stays where it belongs: with you.

DFC Reference: *Right #28 (Privacy Engineering Standard)*

7.5 AI-Assisted Dispute Resolution System

For disputes, claims, or appeals arising from the Vigilance Layer or other Platform actions, RAE provides an AI-Assisted Dispute Resolution system as an efficient first step:

Step 1: Customer Service. Submit your concern to customer service for initial resolution.

Step 2: AI-Assisted Review. If unresolved after customer service, the AI-Assisted Dispute Resolution system evaluates both sides and issues a proposed resolution. For routine disputes (marketplace disputes, fee questions, feature access), the resolution becomes binding unless either party objects within 7 days of receipt (the "objection window"). If no objection is received within 7 days, the resolution is final and binding on both parties. For disputes involving account suspension, content removal, or access to core services, the objection window is extended to 14 days and the user is explicitly notified that human review is available at no cost. If either party objects within the applicable objection window, the matter automatically escalates to human review at the appropriate fractal governance level.

Step 3: Human Escalation. If either party objects to the AI-proposed resolution within the applicable objection window, the matter proceeds to human review at the appropriate fractal governance level.

Step 4: External Resolution. If internal processes are exhausted, external dispute resolution proceeds as described in Section 15.

The AI-Assisted Dispute Resolution system is transparent about its reasoning, subject to human oversight at every stage, and compliant with applicable requirements for meaningful human review in automated decision-making processes. For any dispute that results in account suspension, content removal, or restriction of access to core services, you have the right to request and receive review by a qualified human decision-maker, not solely by an automated system. This right applies regardless of whether you have objected within the standard objection window.

This presumptively binding model will be introduced following an initial testing and feedback period during which all resolutions remain non-binding unless mutually accepted. The transition from testing to presumptive binding will be communicated to users with at least 30 days notice and is subject to community governance review through the Voice system.

Regulatory Alignment: *EU Digital Services Act Article 20, EU AI Act Article 14 (Human Oversight)*

8. Privacy, Data Protection, and Consent

8.1 Privacy Architecture

RAE's privacy architecture is not a policy bolted on after the fact. It is the engineering foundation of the Platform. User data is stored in user-controlled encrypted storage. The Platform has no persistent access to your personal data except as reasonably necessary for operations, safety, security, or legal compliance. Operational telemetry required to maintain and improve Platform performance (error logs, latency metrics, system health data) is collected separately from sovereign user data, is not linked to your identity, and is governed by the Privacy Policy. All storage and access is logged and auditable by you at any time. Communications are end-to-end encrypted via Matrix Protocol. Decentralized storage (Filecoin) ensures your data sovereignty is not dependent on RAE's continued existence.

DFC Reference: *Rights #10 (PII Privacy), #13 (Full Deletion on Exit), #28 (Privacy Engineering Standard)*

Regulatory Alignment: *GDPR Articles 25 (Data Protection by Design and Default), 32 (Security of Processing); CCPA/CPRA; Brazil LGPD Article 46*

Because of this design, 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 (for example, Guide conversation processing or Vigilance Layer behavioral pattern analysis), that processing operates on the minimum data necessary, is logged, and is auditable by you. The only exception to these protections is lawful due process with notification to you, and even then only the narrowest data compelled by a court of competent jurisdiction.

8.2 Consent Framework

All data collection, algorithmic profiling, and feature enrollment require your affirmative opt-in. No pre-checked boxes. No bundled consents. No dark patterns. Every consent you grant is as easy to revoke as it was to give. If you opted in to something, you can opt out with the same number of steps, in the same interface. Your Guide manages your consent settings and can explain them to you at any time.

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

Consent management is supported by automated architectural features, including immutable consent logs stored in your sovereign encrypted storage and periodic AI-assisted scans of consent flows performed by your Guide. These mechanisms ensure that all consents and revocations are accurately recorded, auditable by you at any time, and processed with minimal manual intervention, while maintaining full compliance with the Consent Simplicity Standard (DFC Right #16). You may request a consent audit summary from your Guide at any time.

8.3 Government Data Requests

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)*

8.4 International Data Transfers

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. RAE maintains compliance with applicable data transfer mechanisms including EU Standard Contractual Clauses, UK International Data Transfer Agreements, and equivalent frameworks.

Regulatory Alignment: *GDPR Chapter V (Transfers to Third Countries), UK Data Protection Act 2018, APEC Cross-Border Privacy Rules*

8.5 Data Breach Notification

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 Article 33–34, CCPA §1798.150, NIS2 Directive (EU)*

8.6 User Audit Rights

You have the right to verify that RAE's privacy commitments are real. This right operates at two levels:

Personal audit: You may request a personal audit of your own data at any time through your Guide. This includes: a summary of all consents you have granted and revoked (from the immutable consent logs in Section 8.2); a log of every access to your sovereign data by any Platform system; a record of any Vigilance Layer signals processed in relation to your account; and confirmation that no unauthorized access has occurred. Personal audits cover data retained under the Platform's data retention policy (as detailed in the Privacy Policy) and are provided at no cost.

Independent audit: You may commission an independent privacy audit of your own data, conducted by a qualified auditor of your choosing, at your own expense. RAE will provide reasonable cooperation with the auditor, including access to relevant system logs and architecture documentation, subject to: (a) confidentiality protections for Platform proprietary technology, trade secrets, and security controls; (b) protections for data relating to other users; and (c) reasonable scheduling and scope limitations. RAE will not obstruct, delay, or condition cooperation on unreasonable terms.

In addition, 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.

DFC Reference: *Rights #28 (Privacy Engineering Standard), #10 (PII Privacy)*

Regulatory Alignment: *GDPR Article 15 (Right of Access), Article 28(3)(h) (Audit Rights), EU AI Act Article 72 (Obligations of Providers)*

9. Marketplace Terms

9.1 Marketplace Economics

The RAE Marketplace charges a platform fee as set forth in the Marketplace Policy from time to time, transparently disclosed on every receipt, every time, no exceptions. There is no artificial suppression of listings conditioned on payment; rankings may reflect quality, compliance, and user-selected preferences. Opt-in advertising is available: sellers can advertise; buyers choose whether to see ads and are compensated as set forth in the applicable compensation policy from time to time.

For agent-mediated transactions, the platform fee is calculated as a percentage (α) of the merchant marketing discount redirected to the buyer. Every receipt discloses: the baseline price, the merchant's marketing discount, the platform's share of that discount, and the buyer's net savings. The buyer's transaction price is always lower than the baseline price.

▶ **DFC Reference:** *Right #30 (Marketplace Transparency Standard)*

9.2 Product Listings

Sellers are responsible for the accuracy of product descriptions and pricing. RAE provides community-governed quality control through New, Recommended, Whitelist, and Blacklist systems. RAE may remove listings that violate these Terms or applicable law.

9.3 Payment and Billing

RAE uses third-party payment processors. Separate terms and policies from those processors may apply. You represent that you are authorized to use any payment method you provide. All applicable fees are disclosed before you complete any transaction.

9.4 Subscriptions

Some Services may be offered on a subscription basis. Subscriptions auto-renew unless canceled before the end of the current billing cycle. Cancellation takes effect at the next billing cycle. RAE provides clear cancellation mechanisms with the same number of steps required to subscribe (DFC Right #16).

9.5 Taxes

You are responsible for all applicable taxes, duties, or fees arising from your purchases or sales. RAE will assist with tax reporting where required by law.

9.6 Introduction Fees

Brands may pay users directly for one-on-one introductions, with the Platform receiving a fee as set forth in the Marketplace Policy. You set the terms. Your Guide handles negotiations. The profit goes to you. You decide which brands can approach you.

10. User Conduct and Community Standards

10.1 Prohibited Activities

You agree not to: violate any applicable law or regulation; post or share content that is defamatory, obscene, threatening, or constitutes exploitation of minors; engage in harassment, bullying, or threatening behavior; interfere with the security or operation of the Platform (hacking, phishing, spamming, deploying bots); use the Platform for unauthorized commercial activity; attempt to create multiple User accounts (One Real Person Rule); use the Platform to coordinate inauthentic behavior; send bulk unsolicited messages, spam, scams, phishing links, or pyramid schemes; use automated means (bots, scripts, or external agents) to artificially amplify reach, manipulate engagement, or harass others, except as explicitly authorized by your own sovereign Rebel Agent settings; or promote, facilitate, or engage in violence, terrorism, child exploitation, or other serious criminal activity.

10.2 Content Moderation

Content moderation on RAE is community-governed. Moderation thresholds are set by community vote at the appropriate fractal level. RAE reserves the right to remove content that violates applicable law

regardless of community standards. In response to urgent security, legal, or safety issues, RAE may temporarily override community-set thresholds or rules, with time-bound community review within 30 days of the override. If a conflict exists between community thresholds and legal compliance or platform security, RAE may act immediately to comply with law or mitigate risk, then seek governance review. The escalation process is: Note, Warn, Instruct, Counsel, Fine, Mute, Suspend, Ban. You always have the right to appeal, including through the AI-Assisted Dispute Resolution system described in Section 7.5.

10.3 No Retaliation

RAE will not retaliate against users who advocate for migration to other platforms, for regulatory action, or for collective action of any kind. This is a foundational architectural commitment, not a policy that can be changed without community governance approval. This commitment does not prevent reasonable enforcement of these Terms for conduct that constitutes coordinated inauthentic behavior, harassment, or violation of applicable law.

▶ **DFC Reference:** *Right #23 (Anti-Retaliation Provision)*

11. User-Generated Content and Intellectual Property

11.1 Your Content, Your Ownership

You retain full ownership of all content you create, upload, or post on the Platform ("User Content"). RAE does not claim any license beyond what is strictly necessary to display your content within the Platform as you have directed. Specifically, you grant RAE a limited, non-exclusive license to display, distribute, and technically process your content solely for the purpose of operating the Platform features you have elected to use. This license terminates immediately when you delete the content or leave the Platform.

▶ **DFC Reference:** *Right #36 (Creator Ownership Standard)*

11.2 Departure from Legacy Platform Terms

For clarity: RAE does not claim a worldwide, royalty-free, sublicensable, or transferable license to your content. RAE does not use your content for marketing purposes without your explicit, separate consent. RAE does not retain your content after you leave the Platform.

11.3 Responsibility for Content

You are responsible for your User Content and the consequences of sharing it. RAE does not endorse or guarantee the accuracy of content posted by other users.

11.4 Copyright Claims

If you believe your copyrighted work has been posted without authorization, notify us in accordance with the Digital Millennium Copyright Act (DMCA) or applicable local copyright law by contacting dmca@rebelalliance.earth. Provide: identification of the copyrighted work; identification of the allegedly infringing material; your contact information; a good-faith belief statement; and an accuracy statement under penalty of perjury.

11.5 RAE Intellectual Property

The Platform's proprietary technology, including the Values RAG engine, Fractal Permission Function, Zeitgeist Engine, and related systems, trademarks, logos, and design elements are owned by or licensed to Raindrop, LLC. You are granted a limited, non-exclusive, non-transferable license to access and use the Platform for personal or internal business purposes subject to these Terms.

11.6 Feedback

If you provide suggestions or feedback about the Platform, RAE may use that feedback to improve the Services. Where feedback leads to specific product features, RAE will acknowledge the contribution through the community recognition system.

12. Governance and Collective Decision-Making

12.1 Fractal Governance

RAE operates a fractal governance system scaling from groups of 12 at the Family level through nine nested levels to the Council (global) level. All governance decisions carry sunset clauses. Representatives are elected, not appointed. Appeals always escalate to the next layer. No single group holds unchecked power. This is enforced architecturally.

12.2 Community-Governed Standards

Content moderation thresholds, platform feature priorities, and certain policy decisions are subject to community governance through the Voice system. RAE retains authority over matters of legal compliance, platform security, and the foundational rights established by the Digital Fairness Code. DFC rights are not subject to override by community vote. In emergencies (systemic security threats, legal compliance requirements, or imminent safety risks), RAE may act first and seek governance review within 30 days, consistent with the emergency procedures described in Sections 2.2 and 10.2.

12.3 Self-Governing Communities

Communities may establish self-governing platform instances with their own rules and moderation standards, provided they do not violate these Terms, applicable law, or the Digital Fairness Code.

> **DFC Reference:** *Right #21 (Platform Sovereignty Right)*

13. Disclaimers, Limitations, and Liability

13.1 Service Availability

RAE strives to provide uninterrupted, secure, and error-free Services. However, the Services are provided on an “as available” basis. We do not warrant that the Services will be uninterrupted, error-free, or that defects will be corrected within a specific timeframe. We do warrant that we will use commercially reasonable efforts to maintain service availability and to correct material defects promptly.

13.2 Limitation of Liability

To the fullest extent permitted by applicable law, Raindrop, LLC and its affiliates, directors, officers, employees, and agents shall not be liable for any indirect, incidental, special, consequential, or exemplary damages, including but not limited to loss of profits, revenue, or data, even if advised of the possibility of such damages. Our total liability for any claim arising out of or related to these Terms shall not exceed the greater of: (a) the amount paid by you for accessing the Services in the 12 months preceding the event giving rise to liability; or (b) $100 USD.

Some jurisdictions do not allow the exclusion or limitation of certain warranties or liabilities. In those jurisdictions, our liability is limited to the maximum extent permitted by law. Nothing in these Terms limits

our liability for death, personal injury caused by negligence, fraud, or any matter for which liability cannot lawfully be excluded.

> **Regulatory Alignment:** *EU Consumer Rights Directive, UK Consumer Rights Act 2015, Australian Consumer Law*

13.3 Indemnification

You agree to defend, indemnify, and hold harmless Raindrop, LLC, its affiliates, and their respective directors, officers, employees, and agents from claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of your breach of these Terms, your User Content, your violation of any law, or your misuse of the Services. This indemnification obligation does not apply to claims arising from RAE's own negligence or breach of these Terms.

14. Termination and Account Closure

14.1 Termination by You

You may terminate your account at any time via your Guide, through account settings, or by contacting support. Upon termination at your request: you may export all your data in machine-readable format within 72 hours; complete data deletion occurs within 30 days, independently auditable; your Digital Config and Personal RAG are returned to you or destroyed at your election; your User Content is deleted unless you have exported it.

14.2 Termination by RAE

RAE may suspend or terminate your access to the Services if you materially breach these Terms, engage in illegal activity, or pose a genuine safety threat to other users. Before permanent termination, RAE will provide notice and an opportunity to cure the breach where feasible, except in cases of illegal activity or imminent safety threats. You always retain the right to export your data during any suspension period.

14.3 Effect of Termination

Upon termination, the rights granted to you under these Terms cease. However, your data rights (export, deletion, portability) survive termination. All disclaimers, limitations of liability, and indemnification obligations survive termination. RAE's obligations regarding your data destruction are binding and auditable.

14.4 Deleted User Database

When a User account is permanently closed, the departure is logged (not your data) in a Deleted User database. If you wish to return, a vetting process and explanation are required. Your data is not retained. Bans are reviewable and reversible through the dispute resolution process in Section 15, and prior Deleted User status does not automatically prejudice future participation if the original closure is reversed on appeal.

15. Dispute Resolution and Governing Law

15.1 Governing Law

These Terms shall be governed by and construed in accordance with the laws of the Commonwealth of Puerto Rico, without regard to conflict of law principles. For users outside the United States, to the extent required by mandatory local law, the mandatory consumer protection laws of your jurisdiction of residence shall also apply.

> **Regulatory Alignment:** *Rome I Regulation (EU) for consumer contract choice of law; local mandatory consumer protection laws are preserved*

15.2 Dispute Resolution Process

Before initiating formal proceedings, both parties agree to attempt resolution through the following process:

Step 1: Customer Service. Submit your concern to customer service for initial resolution.

Step 2: AI-Assisted Review. If unresolved, the AI-Assisted Dispute Resolution system (described in Section 7.5) evaluates both sides and issues a proposed resolution. The resolution becomes presumptively binding subject to the objection windows described in Section 7.5 (7 days for routine disputes, 14 days for account/content/access disputes).

Step 3: Mediation. If either party objects to the AI-proposed resolution, the matter proceeds to mediation by a mutually agreed mediator within 30 days.

Step 4: Arbitration or Litigation. If mediation fails, either party may pursue binding arbitration or litigation as described below.

15.3 Arbitration

Either party may elect binding arbitration under the American Arbitration Association rules, applying Puerto Rican law. Each party bears its own costs and attorneys' fees unless the arbitrator determines otherwise. Nothing in this clause prevents you from filing a complaint with your local consumer protection authority or data protection authority. EU users retain the right to bring claims before the courts of their member state of domicile.

> **Regulatory Alignment:** *EU Consumer ADR Directive (2013/11/EU), ODR Regulation (524/2013)*

15.4 Class Action Waiver

You and RAE agree that any dispute resolution proceedings will be conducted on an individual basis and not as part of a class, consolidated, or representative action. You waive any right to participate in a class action lawsuit or class-wide arbitration against RAE. This waiver exists to protect the Platform's ability to serve all users — class action litigation costs can be existential for a mission-driven platform and would ultimately harm the community the Platform exists to serve.

This waiver does not limit your right to: file individual claims through the dispute resolution process in Section 15.2; file complaints with your local consumer protection authority or data protection authority; seek individual injunctive relief in any court of competent jurisdiction; or organize collectively through the Platform's governance systems to negotiate changes to these Terms under DFC Right #03 (Collective Bargaining). If this class action waiver is found unenforceable in your jurisdiction, the remainder of this arbitration agreement remains in full force.

> **Regulatory Alignment:** *Note: Some jurisdictions (including certain EU member states) may not enforce class action waivers. In those jurisdictions, this waiver applies to the maximum extent permitted by applicable law. EU users retain the right to participate in representative actions where mandated by the EU Representative Actions Directive (2020/1828) or applicable member state implementation.*

15.5 Venue

Any legal action not resolved through the process above shall be filed in the courts located in San Juan, Puerto Rico, and you consent to personal jurisdiction in such courts, except where mandatory local law requires a different venue.

16. Open Protocols and Interoperability

RAE is committed to open interoperability. As the Platform grows, RAE will support open protocols for data exchange (including ActivityPub for social federation). User data portability is guaranteed in open, interoperable formats on demand. The Platform's communication layer uses Matrix Protocol with end-to-end encryption. Federated social features leverage PeerTube, Pixelfed, and ActivityPub.

- **DFC Reference:** *Right #22 (Open Protocol Right)*
- **Regulatory Alignment:** *EU Digital Markets Act Article 7 (Interoperability for Messaging), EU Data Act*

17. General Provisions

17.1 Entire Agreement and Supplemental Feature Terms

These Terms, together with the Privacy Policy, Acceptable Use Policy, Marketplace Policy, Compensation Policy, Community Standards, and any Supplemental Feature Terms (collectively, the "Supplemental Terms"), constitute the entire agreement between you and RAE regarding your use of the Services.

Supplemental Feature Terms apply only to the specific optional or paid features they describe (for example, Rebel Premium, advanced AI compute tiers, or future Marketplace enhancements) and are incorporated by reference into these Terms. In the event of any conflict between these Terms and a Supplemental Feature Term concerning the use of that specific feature, the Supplemental Feature Term governs that feature. Supplemental Feature Terms will be presented to you clearly before you opt in or subscribe, and you may revoke consent or cancel at any time with the same ease as granting it (DFC Right #16). No Supplemental Feature Term may reduce or override the rights established by the Digital Fairness Code.

17.2 Severability

If any provision of these Terms is found invalid or unenforceable by a court of competent jurisdiction, that provision shall be enforced to the maximum extent permissible, and the remaining provisions remain in full force and effect.

If any provision of a Supplemental Feature Term is found invalid or unenforceable, only that provision of the Supplemental Feature Term is severed. The remainder of the Supplemental Feature Term, these Terms, and all other Supplemental Terms continue in full force and effect. The invalidity of a Supplemental Feature Term provision does not affect the validity of these core Terms, nor does the invalidity of a core Terms provision affect the validity of any Supplemental Feature Term except to the extent that the Supplemental Feature Term directly depends on the invalidated provision.

17.3 No Waiver

Failure by RAE to enforce any provision of these Terms shall not constitute a waiver of that or any other provision.

17.4 Assignment

You may not assign or transfer your rights or obligations under these Terms without our prior written consent. RAE may assign its rights and obligations under these Terms in connection with a merger, acquisition, or sale of all or substantially all of its assets, provided the assignee agrees to be bound by these Terms including all DFC commitments.

17.5 Force Majeure

RAE shall not be liable for any failure or delay in performance due to circumstances beyond its reasonable control, including natural disasters, acts of government, Internet infrastructure failures, or pandemic-related disruptions.

17.6 Accessibility

RAE is committed to making the Platform accessible to users with disabilities. We comply with WCAG 2.1 Level AA standards and are working toward AAA compliance. If you encounter an accessibility barrier, please contact accessibility@rebelalliance.earth.

> ▶ **Regulatory Alignment:** *EU Web Accessibility Directive (2016/2102), US ADA, Section 508*

17.7 Enterprise Survivability

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

18. Contact Information

For questions about these Terms, your rights, or the Services:

General Inquiries: admin@rebelalliance.earth
Privacy and Data Requests: privacy@rebelalliance.earth
Copyright Claims: dmca@rebelalliance.earth
Accessibility: accessibility@rebelalliance.earth
Legal and Compliance: legal@rebelalliance.earth

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*

Appendix A: Digital Fairness Code Compliance Map

The following table maps each DFC Right to the section of these Terms that implements it.

DFC #	RIGHT	TERMS SECTION(S)
#01	Algorithmic Transparency	1.6, 6.2
#02	Data Portability	1.1, 1.4, 14.1
#03	Collective Bargaining	1.7
#05	Value-Aligned AI Disclosure	6.2
#06	Right to Exit	1.4, 14.1
#07	Right to Be Forgotten	1.5, 14.1
#08	Right to Portability	1.4, 16
#09	Right to Opt In	8.2
#10	Right to PII Privacy	1.1, 8.1
#12	Right to Compensation	1.9, 9.6
#13	Full Deletion on Exit	1.4, 1.5, 14.1
#14	Plain Language Requirement	Preamble, 2.3
#15	Dark Pattern Prohibition	Preamble, 8.2
#16	Consent Simplicity Standard	Preamble, 8.2, 9.4
#19	Coordinated Migration Rights	1.7
#20	Platform Neutrality in Organizing	1.7
#21	Platform Sovereignty Right	12.3
#22	Open Protocol Right	16
#23	Anti-Retaliation Provision	1.7, 10.3
#24	Universal Jurisdiction Framework	1.10
#25	Digital Colonialism Provision	1.10
#26	Decentralized Identity Right	1.2
#27	Self-Sovereign Identity Standard	1.2
#28	Privacy Engineering Standard	7.4, 8.1, 8.6
#29	Government Transparency Mandate	8.3
#30	Marketplace Transparency Standard	9.1
#31	Minor Protection Standard	3.3
#32	Algorithmic Governance Right	1.6, 12.2
#33	AI Agent Sovereignty	1.3, 6.1
#34	Digital Config Right	1.2, 4.2

#35	AI Risk Classification	6.3
#36	Creator Ownership Standard	1.8, 11.1
#37	Algorithmic Wellbeing Standard	7.3
#38	Crisis Response Obligation	7.3
#39	Minor Wellbeing Standard	3.3, 7.3

Appendix B: Global Regulatory Compliance Summary

RAE is designed for global operation. The following summarizes the key regulatory frameworks these Terms are designed to comply with:

JURISDICTION	KEY FRAMEWORKS
European Union	GDPR, Digital Services Act, Digital Markets Act, EU AI Act, eIDAS 2.0, Consumer Rights Directive, NIS2 Directive, Consumer ADR Directive
United Kingdom	UK GDPR, Data Protection Act 2018, Online Safety Act, UK Consumer Rights Act 2015, Age Appropriate Design Code
United States	CCPA/CPRA (California), COPPA, FTC Act §5, ADA, State privacy laws (Virginia CDPA, Colorado CPA, Connecticut CTDPA, etc.)
Brazil	LGPD (Lei Geral de Proteção de Dados)
Canada	PIPEDA, AIDA (Artificial Intelligence and Data Act, pending)
Australia	Privacy Act 1988, Online Safety Act 2021, Australian Consumer Law
South Korea	PIPA (Personal Information Protection Act)
Japan	APPI (Act on the Protection of Personal Information)
India	Digital Personal Data Protection Act 2023
Africa	AU Convention on Cyber Security, Nigeria NDPR, South Africa POPIA, Kenya DPA
ASEAN	ASEAN Framework on Digital Data Governance (member state implementations)
International	FATF AML/KYC Recommendations, OECD AI Principles, WCAG 2.1 Accessibility, UN Convention on the Rights of the Child

By using the Services, you acknowledge that you have read, understood, and agree to these Terms and Conditions.

These Terms are a living document. They evolve with the Platform, with your governance decisions, and with the law. They are always available in plain language at rebelalliance.earth/terms.