LEGACY BUDDY

COMPLIANCE FRAMEWORK

Complete Regulatory & Legal Compliance Reference

Version 1.0 - Effective: March 2026
Jurisdiction: Tennessee (Governing Law) | Operations: All 50 U.S. States
Prepared by: Legacy Buddy, LLC | legal@legacybuddy.com

CONFIDENTIAL - FOR INTERNAL USE AND AUTHORIZED INVESTOR REVIEW ONLY

SECTION EXECUTIVE SUMMARY

Legacy Buddy is a Tennessee-governed generational wealth and estate planning SaaS platform serving all 50 U.S. states. The platform provides three core services: (1) self-help document creation tools for Wills, Trusts, and Powers of Attorney; (2) Legacy Lens™, an AI-powered wealth visualization and readiness scoring engine; and (3) Legacy Counsel, an attorney and financial advisor marketplace. This document enumerates every compliance obligation the company has identified, the regulatory framework requiring it, and the specific measures implemented or planned to satisfy it.

Legacy Buddy operates with a compliance-first architecture. Legal compliance is not treated as a post-launch risk mitigation exercise but as a foundational design constraint embedded in every product, financial, and operational decision. This framework is reviewed quarterly and subject to ongoing attorney oversight.

COMPLIANCE POSTURE SUMMARY
Total Compliance Areas Identified: 8 major categories, 34 specific obligations
Governing Law: State of Tennessee | Platform Jurisdiction: All 50 U.S. States
Outside Legacy Counsel: Pete Kennedy, Graves Dougherty Hearon & Moody (UPL Lead)
Security Standard: SOC 2 Type II (in progress) | Encryption: AES-256 at rest / TLS 1.3 in transit
Data Privacy: CCPA/CPRA compliant | GLBA Safeguards Rule: Applicable (financial data)
Attorney Marketplace: Flat platform fee model - no percentage of legal fees (ABA Rule 5.4(a) compliant)
Document Automation: Self-help tool with attorney-reviewed templates - not a law firm

SECTION 1 MASTER COMPLIANCE STATUS DASHBOARD

The table below provides a high-level view of all compliance obligations, their current implementation status, and the primary obligation each satisfies.

Compliance Area	Status	Key Obligation
UPL / Not a Law Firm	**Active**	Self-help tool positioning; attorney-reviewed templates; UPL disclaimers at all touchpoints
Terms of Service (ToS)	**Active**	22-section ToS governing all users, governing law Tennessee, binding arbitration
Privacy Policy	**Active**	CCPA/CPRA, GLBA, 20+ state laws; GPC signal handling; sensitive data disclosure
CCPA / CPRA (California)	**Active**	Data rights portal, opt-out links, ADMT disclosures for Legacy Lens™
GLBA Safeguards Rule	**In Progress**	Written info security program, designated security officer, vendor oversight
SOC 2 Type II	**In Progress**	Security, Processing Integrity, Confidentiality, Privacy trust service criteria
ESIGN Act / E-Wills	**Active**	State-by-state will execution routing; electronic consent disclosure
ABA Rule 5.4(a) Fee Sharing	**Active**	Flat platform fee; attorneys never receive % of legal fees; independent contractors
Attorney Verification	**Active**	Bar number verification; annual re-verification; auto-suspend on lapse
COI / Professional Insurance	**Active**	COI collection at onboarding; 5-stage annual renewal reminder engine
FINRA / SEC Financial Advisors	**Active**	FINRA official API verification; SEC IAPD cross-check; bad actor screening
SEC RIA / Investment Adviser Act	**Active**	Legacy Lens™ stays within publisher's exclusion; no personalized investment advice
TCPA (SMS/Telemarketing)	**Active**	Dual separate consent checkboxes; STOP auto-response; consent timestamp logging
CAN-SPAM (Email Marketing)	**Active**	One-click unsubscribe; physical address disclosed; honor within 10 business days
FTC Endorsement Guides	**Active**	Ambassador material connection disclosures; mandatory training and monitoring program
COPPA / Minor Data	**Active**	18+ age gate; minor beneficiary data minimization; no analytics use
HIPAA-Adjacent (Medical POA)	**Active**	Enhanced security controls; not a covered entity (explicit disclaimer)

PCI DSS (Payments)	**Active**	Stripe-managed; no full card number storage; PCI pass-through compliance
IRS 1099-NEC (Ambassador Payouts)	**Active**	W-9 collection before first payment; automated 1099 via Stripe Connect
DMCA / Copyright	**Active**	Designated DMCA agent registered; notice-and-takedown procedures live
ADA / Accessibility	**In Progress**	WCAG 2.1 Level AA target; accessibility statement published
Cookie Policy / GPC	**Active**	Pre-consent cookie banner; GPC signal auto-honor; consent preference center
Data Breach Notification	**Active**	48-hr partner notification; 72-hr CA AG notification for 500+ residents
North Carolina Carve-Out	**Active**	N.C. § 84-2.2 special provisions in ToS; NC Bar registration in progress
White-Label Data Processing (DPA)	**Active**	Controller/processor agreement; tenant isolation; 30-day data portability on exit
Stripe Connect Pass-Through	**Active**	Stripe ToS language in user agreement; credit agency disclosure for connected accounts
Plaid Financial Data Disclosure	**Active**	Pre-connection Plaid disclosure screen; revocation controls; Section 1033 prep
Zillow API Attribution	**Active**	Zestimate® trademark; Zillow logo; 'not an appraisal' disclaimer on all property data
California AI Transparency (SB-942)	**In Progress**	AI-generated content labeled; opt-out mechanism in account settings
Colorado AI Act (SB 24-205)	**In Progress**	Impact assessments documented; transparency disclosures for Legacy Lens™
SAM.gov / OFAC Sanctions	**Active**	Exclusions API check at professional onboarding; OFAC SDN list screening
Ambassador / Affiliate Program	**Active**	FTC-compliant disclosure templates; prohibited practice list; W-9 / 1099-NEC
Tennessee UPL (§ 23-3-101)	**Active**	AG Opinion 02-078 safe harbor; no legal judgment exercised by software
State-Specific Privacy Laws	**In Progress**	VCDPA, CPA, CTDPA, TDPSA and 16 other state laws mapped; rolling implementation

SECTION 2 UNAUTHORIZED PRACTICE OF LAW (UPL) COMPLIANCE

UPL risk is the foundational compliance challenge for any legal document automation platform. Legacy Buddy's entire product architecture is structured to stay categorically within self-help tool boundaries, following the framework established by LegalZoom's S-1 filing and the North Carolina statutory safe harbor.

2.1 Core Positioning: Self-Help Technology Tool

Legacy Buddy is classified under SIC Code 7370 (Computer Programming and Data Processing), deliberately avoiding any legal services classification. The platform provides document creation tools, not legal services. Every product decision is evaluated against this test: does this feature require or appear to require the exercise of legal judgment? If yes, it is not built.

WHAT LEGACY BUDDY IS - AND IS NOT
IS: A self-help document creation tool that populates attorney-reviewed templates based on user-directed inputs
IS: A technology platform that facilitates connections between users and independent licensed attorneys
IS: An AI-powered wealth visualization and goal-setting engine providing informational outputs
IS NOT: A law firm - not licensed to practice law in any jurisdiction
IS NOT: A legal advice provider - does not evaluate individual circumstances or render legal opinions
IS NOT: An attorney-client relationship creator - no communications are protected by privilege

2.2 Attorney-Reviewed Templates

Every document template available on the platform has been reviewed and approved by a licensed attorney prior to deployment. Templates are jurisdiction-specific, incorporating state-specific execution requirements (witness counts, notarization, attestation clauses). Templates are reviewed and updated quarterly or upon any relevant change in applicable state law.

2.3 Disclaimer Architecture

UPL disclaimers are not limited to the Terms of Service. They appear at every legally significant user touchpoint in the product flow:

- Account creation: Affirmative checkbox - 'I understand Legacy Buddy is not a law firm and does not provide legal advice' (non-pre-checked, cannot be skipped)
- Document creation initiation: Inline reminder displayed before first questionnaire question
- Document completion / download: Full UPL disclaimer modal required before download or e-sign
- Smart Review and Legacy Counsel pages: Clear statement that Smart Review checks completeness only, not legal accuracy
- Medical POA documents: Additional disclosure that the document does not constitute medical advice
- Footer of every page: 'Legacy Buddy provides document creation tools - not legal advice'

2.4 Tennessee UPL (Tenn. Code Ann. § 23-3-101)

As the governing state, Tennessee's UPL framework defines the primary compliance obligation. TCA § 23-3-101 defines 'law business' broadly; § 23-3-103(b) makes violation a Class A misdemeanor. Tennessee Attorney General Opinion 02-078 provides the controlling safe harbor: filling in blanks of a form document does not constitute UPL 'assuming the decision concerning what information to place on the form does not require the exercise of legal training, skill, or judgment.' Legacy Buddy's software applies this standard strictly - the platform applies no legal judgment, recommends no legal strategies, and draws no legal conclusions.

2.5 North Carolina Special Provisions (N.C. Gen. Stat. § 84-2.2)

North Carolina is the only state with a specific statute explicitly permitting website-based document automation, contingent on seven conditions. Legacy Buddy has implemented all seven: consumer document preview before purchase; NC-licensed attorney review of all NC-applicable templates; disclaimer that the service is not a substitute for attorney advice; identity and location disclosure; no warranty disclaimer for NC consumers; no out-of-state mandatory venue for NC residents; and an active consumer satisfaction process. NC Bar registration is in progress.

2.6 Lola v. Skadden Safe Harbor

The Second Circuit's 2015 ruling in Lola v. Skadden, 620 F. App'x 37, established that tasks which could be performed entirely by a machine do not constitute the practice of law. Template population based on user inputs - with no human legal judgment applied - falls squarely within this precedent.

SECTION 3 DATA PRIVACY & CONSUMER PROTECTION COMPLIANCE

Legacy Buddy collects sensitive personal information including financial account data (via Plaid), beneficiary information about minors, healthcare directive preferences, property valuations, Social Security Numbers in estate documents, and family structure data. This breadth of sensitive data creates obligations under multiple federal and state privacy frameworks simultaneously.

3.1 Privacy Policy

A comprehensive Privacy Policy is published at legacybuddy.com/privacy covering all required disclosures including: categories of personal information collected; sources of collection (directly from users, automatically via platform, from third parties including Plaid and Zillow); purposes of processing; third-party disclosures; retention periods; consumer rights; and contact information for privacy requests. The policy is updated whenever data practices change and reviewed annually against evolving state law requirements.

3.2 CCPA / CPRA (California Consumer Privacy Act / California Privacy Rights Act)

Legacy Buddy complies with the CCPA as amended by CPRA for California residents. Key implementations:

- 'Do Not Sell or Share My Personal Information' link in website footer - legally required
- 'Limit the Use of My Sensitive Personal Information' link - separate from the above
- Data Rights Request portal in user dashboard: access, delete, correct, and export buttons
- 45-day response SLA for all data rights requests
- Global Privacy Control (GPC) signal auto-detection - tracking scripts blocked when GPC = true
- Sensitive personal information (SSNs, financial account numbers, health data) flagged for enhanced protection
- Automated Decision-Making Technology (ADMT) disclosures for Legacy Lens™ per 2026 CPRA ADMT regulations
- AI opt-out mechanism in account settings; human review escalation path available
- Cybersecurity risk assessments documented and certified by senior executive per CPRA requirement

3.3 Multi-State Privacy Law Compliance

As of 2026, 20+ U.S. states have enacted comprehensive consumer privacy laws. Legacy Buddy's privacy program addresses all active laws including:

State Law	Effective	Key Obligation for Legacy Buddy
CCPA/CPRA (California)	Jan 2020 / Jan 2023	Full compliance - most rigorous regime
VCDPA (Virginia)	Jan 2023	Consumer opt-out rights; data protection assessments
CPA (Colorado)	Jul 2023	GPC signals honored; opt-out of profiling
CTDPA (Connecticut)	Jul 2023	Consent for sensitive data processing
TDPSA (Texas)	Jul 2024	No sale without opt-out notice
FDBR (Florida)	Jul 2024	Additional consumer rights for FL residents

MCDPA (Montana)	Oct 2024	Data minimization; purpose limitation
OCPA (Oregon)	Jul 2024	Comprehensive rights; 45-day response
NHPA (New Hampshire)	Jan 2025	Right to correct; right to delete
NDPA (New Jersey)	Jan 2025	Opt-out of targeted advertising
DPDPA (Delaware)	Jan 2025	Risk assessments for high-risk processing
ICDPA (Iowa)	Jan 2025	Narrower scope; access and delete rights
12+ Additional States	2025–2026	Rolling compliance implementation in progress

3.4 GLBA Safeguards Rule (Gramm-Leach-Bliley Act)

The FTC's expanded interpretation of GLBA may apply to Legacy Buddy given that Legacy Lens™ collects and processes consumer financial nonpublic personal information (NPI) via Plaid. The platform treats GLBA compliance as mandatory and has implemented all required elements of the FTC Safeguards Rule (16 C.F.R. Part 314):

- Designated Qualified Individual (security officer) responsible for the written Information Security Program
- Annual written risk assessments identifying internal and external threats to NPI
- Safeguards for all identified risks: access controls, encryption, multi-factor authentication
- Continuous monitoring and testing of security controls
- Annual penetration testing and bi-annual vulnerability scanning
- Vendor oversight program - all vendors handling NPI must sign Data Processing Agreements
- Incident response plan tested annually via tabletop exercises
- Annual board-level reporting on the Information Security Program
- Annual GLBA privacy notices to consumers disclosing NPI sharing practices

3.5 HIPAA-Adjacent Compliance (Medical POA / Healthcare Directives)

Legacy Buddy is NOT a HIPAA Covered Entity (it is not a healthcare provider, health plan, or healthcare clearinghouse) and this is explicitly disclosed in the Terms of Service and Privacy Policy. However, because the platform collects healthcare directive preferences (Medical POA, living will preferences, end-of-life instructions), enhanced security and data minimization controls are applied to healthcare-adjacent data. The Washington My Health My Data Act and Connecticut consumer health data law apply to non-HIPAA entities collecting health-related data and are incorporated into the platform's privacy controls.

3.6 Minor Beneficiary Data Protection

When users add minor children as beneficiaries or guardians, the platform collects names, dates of birth, and relationship data. Controls applied: data minimization (only information necessary to populate documents is collected); no use of minor data for analytics, AI training, or marketing segmentation; prohibition on selling or sharing minor data; age gate at 18+ for account creation; enhanced access controls on records containing minor beneficiary data.

3.7 Cookie Policy & Global Privacy Control

A cookie consent banner fires before any non-essential scripts load. Essential cookies (session management, security) activate without consent; analytics, marketing, and tracking cookies require affirmative opt-in. GPC browser signals are automatically detected and honored - all tracking is disabled without user prompt when GPC is active. A consent preference center is accessible from the footer at all times. Consent choices, policy version shown, and timestamps are stored for compliance documentation.

SECTION 4 FINANCIAL REGULATIONS — SEC, FINRA & INVESTMENT ADVISER ACT

Legacy Lens™, the platform's AI-powered wealth visualization engine, operates at the intersection of financial technology and investment regulation. The compliance framework for this component is anchored in two established safe harbors that protect informational financial tools from Investment Advisers Act registration requirements.

4.1 Publisher's Exclusion (Section 202(a)(11)(D), Investment Advisers Act of 1940)

Legacy Lens™ is positioned as an informational tool that applies identical analytical methodology to all users. The publisher's exclusion exempts publishers of bona fide financial publications from the investment adviser definition when: (a) advice is general and impersonal, not tailored to individual investment needs; (b) the publication is bona fide (not a tout); and (c) the publication is of general and regular circulation. Legacy Lens™ satisfies all three criteria.

4.2 'Inanimate Tool' / FPL Associates No-Action Letter Safe Harbor

The SEC staff's FPL Associates no-action letter declined enforcement against financial planning software applying objective, non-discretionary criteria - even when the software recommended specific asset allocations based on user inputs including age, risk tolerance, and timeline. Legacy Lens™ operates within this safe harbor by: (a) applying the same scoring methodology (LQ™ algorithm) to all users; (b) never recommending specific securities, funds, or investment products; (c) generating no revenue tied to securities transactions; and (d) including prominent 'not financial advice' disclosures on all outputs.

4.3 Legacy Buddy Is NOT a Registered Investment Adviser

Legacy Buddy, LLC is not registered as an investment adviser with the SEC or any state securities regulator. Legacy Lens™ does not provide personalized investment advice within the meaning of the Investment Advisers Act of 1940 or any applicable state law. All AI-generated wealth insights are informational estimates only. Users are explicitly directed to consult qualified, licensed financial advisers for investment decisions. This disclaimer appears at the Legacy Lens™ dashboard, in the Terms of Service (Section 15), and in all email communications referencing financial estimates.

4.4 Legacy Lens™ AI Output Guardrails

Technical content guardrails prevent Legacy Lens™ from generating outputs that cross the line from information to advice. The AI system is explicitly prohibited from: recommending specific securities, stocks, bonds, ETFs, or mutual funds; providing personalized investment portfolio allocations; advising on specific insurance products; providing tax strategy recommendations; or generating outputs that reference specific financial institutions in a recommendation context. The system may generate: net worth estimates; debt payoff projections; illustrative wealth growth scenarios; general financial literacy information; and Legacy Quotient™ readiness scores.

4.5 Financial Advisor Verification - FINRA & SEC

Financial advisors listed in the Legacy Counsel marketplace are verified through the following infrastructure:

- FINRA Official API (developer.finra.org): OAuth 2.0 authenticated access to registration validation, disciplinary records, and the individualDelta dataset for annual re-verification
- SEC IAPD bulk data: Monthly cross-reference against Form ADV data (adviserinfo.sec.gov)
- CFP Board verification: Manual confirmation of active CFP® certification status
- OFAC SDN List screening: SAM.gov Exclusions API check at onboarding
- OIG LEIE exclusion check: Monthly bulk download cross-reference
- Annual re-verification via FINRA individualDelta dataset: flags any status changes automatically

- Automatic de-listing upon confirmed suspension, revocation, or disqualification

SECTION 5 ATTORNEY MARKETPLACE - ABA RULE 5.4(a) & FEE-SHARING COMPLIANCE

The attorney fee-sharing prohibition under ABA Model Rule 5.4(a) - replicated in every state's professional conduct rules - represents the most consequential compliance risk for any legal tech platform operating an attorney marketplace. Avvo's forced shutdown in 2018 after ethics opinions from eight states demonstrated the consequences of a non-compliant fee structure. Legacy Buddy's marketplace is architected from the ground up to avoid every element of the Avvo model.

5.1 The Avvo Problem - What We Deliberately Avoided

Avvo's fatal flaw was charging attorneys a 'marketing fee' that varied with the value of each legal service rendered. New York NYSBA Opinion 1132, New Jersey Joint Opinion (ACPE 732), Virginia Legal Ethics Opinion 1885, and five additional state bar opinions all found this structure violated Rule 5.4(a) because the fee - regardless of label - was tied to legal fee amounts. The Virginia opinion established the 'substance over form' doctrine: any payment that 'has any relation to the amount of the legal fee' constitutes unethical fee sharing.

5.2 Legacy Counsel Fee Structure - The Compliant Model

Legacy Buddy charges attorneys a flat technology platform fee for marketplace access. This fee is:

- Fixed in amount - the same regardless of whether the attorney handles a $200 document review or a $10,000 trust administration
- Charged for platform access - not per referral, not per matter, not per client retained
- Unrelated to legal fee value - there is no mechanism by which the platform fee correlates with what the attorney earns
- Charged whether or not the attorney is engaged by any particular client

The attorney-client fee relationship is entirely separate from the platform fee. Clients pay attorneys directly. Legacy Buddy never holds, intermediates, or takes a percentage of legal fees. This structure is modeled on the LegalZoom Legal Advantage plan, explicitly distinguished as compliant in the NJ Joint Opinion.

5.3 Non-Discretionary Matching Criteria (NYSBA Opinion 1131 Safe Harbor)

NYSBA Ethics Opinion 1131 established a safe harbor for attorney referral services that match clients using mechanical, non-discretionary criteria. Legacy Counsel matches users with available attorneys based on: geographic availability and bar admission state; practice area (estate planning, trusts); availability for the requested service type; and calendar availability. The platform does not rank, endorse, or recommend attorneys as 'best,' 'top-rated,' or 'qualified.' No satisfaction guarantees tied to attorney performance are offered.

5.4 Professional Services Agreement - Key Protective Clauses

Every attorney on the Legacy Counsel marketplace executes a Professional Services Agreement that establishes:

- Attorney as independent contractor - not employee, agent, or representative of Legacy Buddy
- Attorney-client relationship exists exclusively between the attorney and the end user
- Legacy Buddy does not supervise, direct, or control legal services provided
- Attorney retains full professional independence and responsibility for all legal work
- Attorney must maintain active bar membership in all states where they serve clients

- Attorney must maintain professional liability insurance (minimum $1M per claim, $2M aggregate for attorneys; $500K/$1M for financial advisors)
- Annual re-verification of bar status and insurance required as condition of continued listing
- Automatic suspension upon any confirmed disciplinary action, license suspension, or insurance lapse

5.5 Smart Review Fee Structure

The $199 Smart Review service is structured as a technology platform fee payable to Legacy Buddy for document review infrastructure - not a legal service fee. The reviewing attorney's compensation is structured as a flat access fee paid by the attorney to the platform, not as a share of the $199 charged to the user. Review scope is explicitly limited to completeness, internal consistency, and typographical errors - not legal accuracy or suitability assessment.

5.6 Bar Verification Infrastructure

Attorney bar verification at onboarding and on an annual basis covers:

- Primary source verification against each state bar's official online directory
- Discipline history check including suspensions, censures, disbarments, and public reprimands
- ABA National Lawyer Regulatory Data Bank ($10/name) at onboarding for cross-jurisdictional discipline history
- Annual automated re-verification via state bar websites (scheduled job, all 51 jurisdictions)
- States with no online search (New Hampshire, South Dakota) handled via phone verification
- States allowing attorney opt-out (Oklahoma, Virginia) handled via supplementary manual verification
- Immediate auto-suspension upon detection of active disciplinary status or expired license
- Third-party aggregator partnership (Certemy or Evident) for continuous monitoring

SECTION 6 COMMUNICATIONS & MARKETING COMPLIANCE

6.1 TCPA - Telephone Consumer Protection Act (47 U.S.C. § 227)

The TCPA imposes strict requirements on SMS marketing communications, with statutory damages of $500–$1,500 per violation per message. Legacy Buddy's TCPA compliance infrastructure includes:

- Dual separate consent checkboxes at account creation: one for transactional SMS (OTP, security alerts, document notifications) and one for marketing SMS - neither pre-checked
- Marketing SMS consent language: 'By checking this box, you consent to receive marketing texts from Legacy Buddy. Consent is not required to purchase. Message and data rates may apply. Reply STOP to unsubscribe.'
- STOP/HELP auto-response system via AWS SNS/Twilio - immediate removal from marketing lists upon STOP
- Consent timestamp log stored in database: when consent was given, policy version displayed, IP address
- No marketing SMS before 8:00 AM or after 9:00 PM in recipient's local timezone - timezone detection in dispatch logic
- 10DLC registration completed for all business text messaging campaigns
- CTIA-compliant SMS template library across 8 message categories

6.2 CAN-SPAM Act (15 U.S.C. §§ 7701–7713)

All commercial email communications comply with CAN-SPAM requirements: clear identification as advertising where applicable; physical mailing address of Legacy Buddy, LLC in every marketing email; functional one-click unsubscribe mechanism; opt-out requests honored within 10 business days; no deceptive subject lines or 'from' addresses; subject lines accurately reflect email content.

6.3 FTC Endorsement Guides - Ambassador Program (16 C.F.R. Part 255)

The FTC revised its Endorsement Guides in June 2023, with civil penalties up to $51,744 per violation. Legacy Buddy's Ambassador Program Agreement implements full compliance:

- Mandatory disclosure of material connection on every piece of promotional content - per-post, not a single site-wide disclaimer
- Compliant disclosure language provided: 'Paid partnership with Legacy Buddy' or 'I earn commissions for purchases through this link'
- Non-compliant labels explicitly prohibited: '#ambassador' and '#partner' alone are insufficient per FTC guidance
- Disclosure placement requirements: above the fold on Instagram, verbal at start of YouTube videos, top of blog posts
- Legacy Buddy maintains a training, monitoring, and compliance program: disclosure templates provided; periodic content search for non-compliant ambassadors; corrective action procedures
- Prohibited marketing practices: no claims about legal outcomes; no fake or AI-generated reviews (FTC August 2024 rule); no bidding on Legacy Buddy trademarks in paid search
- W-9 collected before any first payment; 1099-NEC filed for all payouts exceeding IRS threshold
- Ambassador Program Agreement filed with outside counsel for review

SECTION 7 INFORMATION SECURITY & DATA INFRASTRUCTURE COMPLIANCE

7.1 SOC 2 Type II Certification (In Progress)

Legacy Buddy is pursuing SOC 2 Type II attestation covering four Trust Service Criteria: Security (mandatory), Processing Integrity (document generation accuracy), Confidentiality (estate documents, SSNs, financial records), and Privacy (PII lifecycle management). The audit is being conducted using Drata for continuous automated control monitoring. SOC 2 Type II is required by institutional partners (financial institutions, insurance companies, law firms) and is expected to be completed within 12–18 months.

- SOC 2 Type I completion: Q3 2026 (target)
- SOC 2 Type II completion: Q1 2027 (target)
- Continuous monitoring platform: Drata
- Audit firm: [To be selected from Big 4 or top-tier regional CPA firm]

7.2 Encryption & Access Controls

- All documents and user data encrypted at rest using AES-256
- All data in transit encrypted using TLS 1.3
- Role-based access controls (RBAC) with principle of least privilege
- Multi-factor authentication (MFA) required for all user accounts and all staff access to production systems
- Immutable audit logs for all document access, modification, and sharing events
- Zero-trust network architecture for internal systems

7.3 AWS Infrastructure Security

Legacy Buddy is built on AWS (us-east-1) with the following security controls:

- AWS Lambda (serverless) - no persistent server attack surface
- Aurora Serverless (PostgreSQL) + DynamoDB - encrypted at rest with AWS KMS
- S3 + Glacier - AES-256 server-side encryption; versioning enabled
- Amazon Cognito - identity management with SSO/SAML support
- CloudWatch - real-time monitoring, alerting, and log retention
- AWS Step Functions + EventBridge - workflow automation with audit trails
- WAF (Web Application Firewall) - OWASP Top 10 protection
- CloudTrail - complete API call logging for compliance and forensics

7.4 Third-Party Vendor Security

All third-party vendors handling user personal information must satisfy Legacy Buddy's vendor security requirements:

- Execute a Data Processing Agreement (DPA) before any data access
- Maintain SOC 2 Type II certification or equivalent (ISO 27001)
- Plaid: ISO 27001, ISO 27701, SOC 2 Type II - AES-256 encryption and tokenization
- Stripe: PCI DSS Level 1 certified - no full card number storage on Legacy Buddy systems
- DocuSign: ISO 27001, SOC 2 Type II, FedRAMP authorized
- AWS: SOC 1/2/3, ISO 27001, PCI DSS Level 1, HIPAA eligible

- Annual vendor security review; immediate notification requirements for security incidents affecting Legacy Buddy data

7.5 Data Breach Notification Compliance

Legacy Buddy maintains breach notification procedures compliant with all 50 state breach notification laws plus applicable federal requirements. Key procedures:

- White-label partner notification: 48–72 hours from confirmed breach
- California AG notification: within 72 hours for breaches affecting 500+ California residents (Cal. Civ. Code § 1798.82)
- All 50 states: notification within applicable state deadline (30–90 days depending on state)
- Consumer notification: clear, plain-language notice with description of incident, data affected, and remediation steps
- Annual tabletop incident response exercise; documented response plan reviewed quarterly

7.6 Document Retention and Deletion

CPRA requires publication of specific retention periods and actual enforcement of those periods. Legacy Buddy's retention schedule:

Data Type	Retention Period	Deletion Method
Estate planning documents	Active subscription + 7 years post-termination	Crypto-shredding (key deletion)
Financial data (Plaid sync)	Active subscription only; deleted within 30 days of cancellation	Hard delete + audit log
Account / identity data	Active account + 3 years post-closure	Hard delete
Marketing / email lists	Until unsubscribe + 1 year	Hard delete
Audit and access logs	5 years (regulatory compliance)	Archival then hard delete
Payment records	7 years (IRS / tax compliance)	Encrypted archival
Ambassador / affiliate records	7 years (IRS / 1099 records)	Encrypted archival

SECTION 8 PLATFORM-SPECIFIC & INTEGRATION COMPLIANCE

8.1 Electronic Signature Compliance - ESIGN Act & State E-Wills Laws

Wills, codicils, and testamentary trusts are expressly excluded from the ESIGN Act's electronic signature validity provisions in approximately 37 states. Legacy Buddy has built state-specific will execution routing logic:

- At document creation, user's state is confirmed via account settings and questionnaire
- States with enacted e-wills legislation (~13–14 states including FL, CO, NV, VA, AZ, IN, UT): electronic execution via DocuSign is offered
- All other states (~37): platform requires print, sign, and witness workflow with state-specific execution instructions displayed
- A prominent in-product warning displays at document completion: 'This document is only valid when signed according to [State]'s requirements'
- Platform prevents users from marking a will as 'complete' without confirming execution method
- E-Sign Consent Disclosure presented before any electronic signature — includes right to paper copies, right to withdraw consent, scope of consent, hardware requirements

8.2 Plaid Financial Data Integration Compliance

Plaid integration requires specific disclosure obligations:

- Pre-connection disclosure screen displayed before Plaid Link opens: 'Legacy Buddy uses Plaid to connect your accounts. Plaid will access your account data on our behalf. View Plaid's privacy policy at plaid.com/legal.'
- 'Manage Connected Accounts' page in user dashboard allows revocation of Plaid access at any time
- Authorization timestamps stored for each Plaid connection
- Re-authorization required every 12 months (CFPB Section 1033 preparation)
- No bank-credential harvesting outside Plaid Link - zero credential storage on Legacy Buddy systems
- Plaid $58M settlement (2022) compliance: no bank-mimicking UI; Plaid identified by name in all disclosures; data minimization applied

8.3 Stripe Payment & Connect Compliance

Stripe's Platform Agreement mandates specific pass-through language, implemented in the Legacy Buddy Terms of Service:

- Stripe Connected Account Agreement and Stripe Terms of Service referenced in user ToS with links
- User authorization for Legacy Buddy to share transaction information with Stripe
- Stripe Privacy Policy linked with statement that personal payment data is processed per Stripe's Privacy Policy
- Credit agency disclosure for connected account (attorney/advisor) onboarding
- PCI DSS compliance via Stripe - no full card numbers stored by Legacy Buddy
- IRS Form 1099-K reporting for Stripe-processed payments where applicable

8.4 Zillow Zestimate® API Attribution

Zillow's API Terms of Use require specific attribution on all property valuations displayed:

- Approved Zillow logo displayed adjacent to all Zestimate® data
- 'Zestimate®' trademark registered mark displayed - not abbreviated as 'Zestimate'

- Link to property details page on Zillow.com
- Copyright notice: '© Zillow, Inc. [Year]'
- Mandatory disclaimer: 'The Zestimate® is Zillow's estimate of a property's market value and is not an appraisal. For estate planning purposes, a certified professional appraisal should be obtained.'
- All Zestimate data displayed as non-removable UI components - cannot be disabled by white-label partners

8.5 DocuSign Electronic Signature Integration

DocuSign is used for electronic signatures on documents where electronic execution is legally permitted. Compliance controls:

- State-specific routing ensures DocuSign is only offered in e-wills-authorized states for testamentary documents
- DocuSign audit trail (certificate of completion) stored with each signed document in Legacy Vault
- DocuSign terms of service incorporated by reference in Legacy Buddy user agreements
- E-Sign consent obtained before any DocuSign workflow is initiated

SECTION 9 COMPLIANCE GOVERNANCE & INFRASTRUCTURE

9.1 Outside Legal Counsel

Legacy Buddy retains specialized outside counsel for each compliance domain:

- UPL / Legal Tech Law: Pete Kennedy, Graves Dougherty Hearon & Moody (Austin, TX) - identified as leading UPL counsel for legal tech platforms
- Data Privacy: [To be retained - CIPP/US certified privacy counsel]
- Employment / Independent Contractor: [Tennessee-licensed employment counsel]
- Securities / Investment Advisers Act: [Securities counsel to review Legacy Lens™ positioning annually]
- All legal documents carry 'DRAFT - FOR ATTORNEY REVIEW' status until reviewed and approved

9.2 Compliance Review Schedule

Activity	Frequency	Owner
Terms of Service & Privacy Policy review	Annual (+ upon material change)	Outside Counsel + CEO
State bar attorney re-verification	Annual (automated)	Engineering + Legal Ops
FINRA advisor re-verification	Annual via individualDelta API	Engineering
COI renewal reminder cycle	Annual (auto-triggered 90 days before expiry)	Platform (automated)
Penetration testing	Annual	Security (3rd party vendor)
Vulnerability scanning	Bi-annual	Engineering / DevSecOps
Privacy Policy vs. state law updates	Quarterly	Privacy Counsel
CCPA Data Protection Risk Assessment	Annual (CPRA requirement)	DPO / Privacy Counsel
SOC 2 audit preparation	Continuous (Drata monitoring)	Engineering / Compliance
Ambassador / affiliate compliance monitoring	Quarterly content search	Marketing / Legal
GLBA Information Security Program review	Annual board-level report	Security Officer / Board
Incident response tabletop exercise	Annual	All departments

9.3 Compliance as Competitive Moat

Legacy Buddy's compliance infrastructure is not merely defensive - it is a primary barrier to entry and a driver of institutional partnership opportunities. Platforms seeking enterprise contracts with financial institutions, insurance companies, and national law firms require SOC 2 Type II, comprehensive privacy programs, and documented regulatory compliance before any agreement can be executed. Building this infrastructure requires 2–3 years and multi-million dollar investment. Competitors entering after Legacy Buddy will face this same timeline, creating a durable structural advantage.

LegalZoom's S-1 articulates this directly: it took seven years from service inception to offer 50-state attorney network coverage. Trust & Will's Series C fundraising explicitly cited SOC 2 and privacy compliance as partnership prerequisites for Northwestern Mutual, UBS, and USAA. Legacy Buddy's compliance investments today directly enable the institutional distribution channel that defines our growth trajectory.

LEGACY BUDDY, LLC | Build. Grow. Pass it on.

legal@legacybuddy.com | www.legacybuddy.com | [Registered Address, Tennessee]