Security Documentation

Version 1.0.3 – November 6, 2025

Audience – Information-security reviewers at large corporations and large law firms evaluating the L.E.G.A.L. GenAI Survey operated by LexFusion Intelligence (the "Service").

*Scope – Collection, transmission, processing, storage, and reporting of survey-response data *only*. No privileged, matter-level or financial data is collected.*

Table of Contents

1. Preface

The following document goes over the security features and methodologies we have implemented in the design of our service. The primary focus of security, with respect to the 'service,' is maintaining data privacy and access security.

Sections 3-4 provide a concise overview of the program flow, the third-party services it uses, and the methods between them to ensure data is kept private and only accessible as we determine and is otherwise completely closed off from the public.

Sections 5-7 provide a more comprehensive look at the technical methods in which our service and the third-party services/APIs in use ensure data privacy and restricted access. This overview will go into the layers of security involved during the development, deployment, and running states of our application. Many of the services mentioned share commonalities in practice of tried and tested approaches to cybersecurity; industry practice dictates these are the best standards to avoid data leaks, unwanted access, data corruption, and various vulnerabilities.

2. Document Metadata

Owner	Casey Flaherty
Revision History	V1.0.03 – Draft – November 6, 2025

*** Revision History: 1 – major version, 0 – standard version update, 03 – minor version updates**

3. Overview

This platform is built using a defense-in-depth architecture exclusively on mature third-party services. It facilitates secure distribution of surveys and analysis of survey data while enforcing strong security standards at every layer. All vendors (Azure, MongoDB Atlas, JotForm, Microsoft, Cloudflare) maintain SOC 2 Type II and/or ISO 27001 certifications with all privileged access requiring MFA. TLS 1.2+ is enforced end-to-end, and all data at rest is encrypted with AES 256, managed by the respective services.

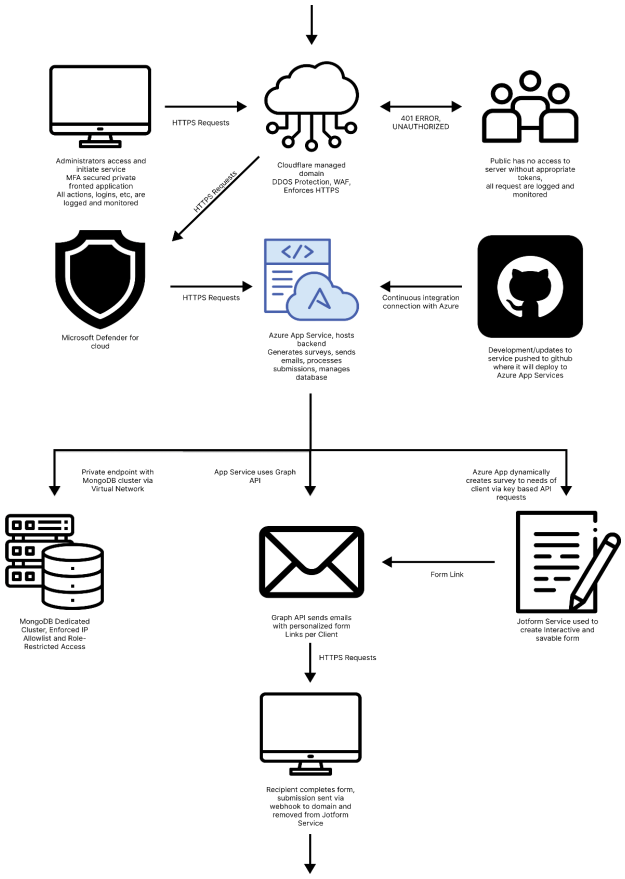
- **Frontend (Tauri + Vite):** Runs as a private desktop app, communicates over HTTPS and WSS, no direct access to sensitive data; all routed through backend.
- **Backend (Node.js on Azure App Service):** Token-based auth with strict middleware checks, sanitization, validation, CORS origin locking, and Azure Defender security headers.
- **Database (MongoDB Atlas - Dedicated Cluster):** Access restricted to Azure Private Link within a Virtual Network, data encrypted at rest (AES-256), and role-based access control (RBAC) and IP allowlists enforced.
- **Email Delivery (Microsoft Graph API):** Uses OAuth2 delegated permissions, TLS enforced for all message transit, domain secured with SPF, DKIM, DMARC.
- **Surveys (JotForm):** Used only to render dynamic forms and collect responses, responses retrieved via secure API and immediately stored to MongoDB and deleted from Jotform upon completion, and admin access via MFA.
- **Network Layer (Cloudflare + Azure VNet):** Cloudflare enforces HTTPS, WAF, DDoS protection, all backend services behind private endpoints with no public exposure, and logs monitored 24/7 for threats; alerts escalate to on-call engineers.

The platform adheres to strict data governance standards, classifying all collected information—including business contact details and survey responses—as CONFIDENTIAL. All data is securely stored and processed exclusively within U.S.-based, enterprise-grade data centers, ensuring compliance with industry best practices for residency and jurisdiction. By relying solely on PaaS and SaaS providers, the system benefits from robust, independently maintained security controls and avoids the operational risks associated with self-hosted infrastructure.

4. System Architecture & Data Flow

Client requests service → Administrator initiates service -> Graph API (HTTPS) personalized links

Respondent → (TLS) → Jotform (survey form) → (Webhook, TLS) → Node.js 22-LTS backend (Azure App Service) → (TLS, VNet-peered) → MongoDB Atlas



5. Component Inventory

This table outlines all third-party services and platforms used across the survey application workflow. Each row identifies a specific component, its role within the system, where it is hosted, the core security features it offers, and any verified certifications that demonstrate adherence to industry standards. The purpose is to demonstrate a mature vendor selection process that prioritizes secure, audited platforms for critical operations like data collection, processing, storage, and delivery.

#	Component	Role in Workflow	Hosting / Service	Primary Security Features	Verified Certifications*
1	JotForm Enterprise	Renders survey forms & captures responses	AWS (multi-region, managed by JotForm)	TLS 1.3, secret token for webhook validation via query param	SOC 2 Type II, ISO 27001, PCI-DSS
2	Azure App Service (Linux) running Node 22-LTS	Validates input, applies business logic, writes to DB, triggers email	Microsoft Azure	Auto-patching, container isolation, Azure Defender, Managed Identity, strict CORS	SOC 1/2/3, ISO 27001, ISO 27017
3	MongoDB Atlas Dedicated Cluster (M30+)	Stores survey data	MongoDB Atlas on Azure	AES-256 at rest, IP allow-list, RBAC, optional field-level encryption, VNet Private Endpoint	SOC 2 Type II, ISO 27001
4	Microsoft Graph API	Sends personalized survey links & reminders	Microsoft 365 SaaS	OAuth2 delegated access, TLS enforcement, SPF/DKIM/DMARC alignment	SOC 2 Type II, ISO 27001
5	Cloudflare DDoS / WAF	Public-facing DNS, TLS termination, DDoS & bot mitigation	Cloudflare Anycast Network	WAF (basic OWASP ruleset), TLS termination, origin restrictions	SOC 2 Type II, ISO 27001
6	GitHub Actions (OIDC-federated)	CI/CD pipeline for IaC and application code	GitHub.com	OIDC tokens to Azure, branch protection, code review enforced	SOC 2 Type II, ISO 27001
7	Azure Monitor & Defender for Cloud	Centralized logging, basic threat detection	Microsoft Azure	Log retention, alerting for known threat patterns	SOC 1/2/3, ISO 27001

6. Data-Lifecycle Control Points

This table maps the full lifecycle of survey data—from collection to deletion—alongside the security controls enforced at each phase. It highlights how the system ensures data confidentiality, integrity, and access control at all key transition points. These controls are both technical (e.g., TLS, schema validation, encryption) and administrative (e.g., access policies, retention schedules), supporting compliance with data protection expectations.

Phase	Controls in Effect
Collection	TLS 1.2 to JotForm; incoming webhook, submission validated against defined schema; least-privilege JotForm API token
Transit	End-to-end encryption (TLS 1.2+); Cloudflare Origin Pull uses mTLS
Processing	Node.js libraries validate JSON schema (Mongoose), drop unexpected fields, and sanitize input against injection
Storage	MongoDB Atlas: AES-256 at rest; IP allow-list; role-based access control (RBAC); daily encrypted backups
Access	Admin UI protected by Azure AD SSO + Conditional Access + MFA; database access gated via bastion host with Just-In-Time access
Deletion	Data purged 30 days after project close via scripted Atlas Data API; backups retained for 90 days

7. Compliance & Assurance Artifact

This table lists external certifications and security audit reports provided by each vendor involved in the system's operation. It serves as evidence that the platform is built on top of independently verified, enterprise-grade infrastructure.

Artifact	Custodian	Availability to Reviewers
SOC 2 Type II report – MongoDB Atlas	MongoDB Inc.	NDA with MongoDB
SOC 1 / SOC 2 Type II – Microsoft Azure	Microsoft	Azure Trust Center (public summary)
SOC 2 Type II – Cloudflare	Cloudflare, Inc.	Available under NDA
SOC 2 Type II – GitHub	GitHub, Inc.	Public SOC 3 + NDA for SOC 2
SOC 2 Type II – Jotform Enterprise	JotForm Inc.	NDA with JotForm
PCI-DSS v4 Attestation – JotForm	JotForm Inc.	Upon request
ISO 27001 certificate – All vendors	Various	Public trust centers

8. Shared Responsibility Matrix

This table defines the division of security and operational responsibilities between third-party cloud vendors and LexFusion Intelligence. It distinguishes which controls are managed by the cloud provider (e.g., physical security, infrastructure patching) and which are owned by the internal application team (e.g., application security, data governance, incident response coordination).

Control Area	Vendor Responsibility	LexFusion Intelligence Responsibility
Physical security of datacenter	Cloud Vendor	–
Hypervisor & infrastructure patching	Cloud Vendor	–
Application code security	–	Secure coding, code review, CI/CD scanning (SAST, DAST)
Survey content & respondent PII	–	Provide accurate input, implement deletion logic on request
Identity governance (internal users)	–	Enforce MFA, least-privilege, role reviews
Data retention & deletion	Backup infrastructure (Atlas)	Define & execute deletion logic; manage retention schedule
Incident response to platform outage	Cloud Vendor primary	Coordinate communication, run business impact analysis

Appendix A – Data Processing Agreement

This Appendix provides a standard Data Processing Agreement (DPA) template, designed to govern the processing of personal data under the GenAI Adoption Survey. The template is aligned with the EU General Data Protection Regulation (GDPR) and other applicable privacy frameworks.

1. Subject Matter and Duration

This Agreement governs the processing of personal data by the Processor on behalf of the Controller in connection with the GenAI Adoption Survey. The duration shall match the term of the underlying engagement.

2. Nature and Purpose of Processing

The Processor shall collect and analyze business contact information and survey responses to produce anonymized analytics for the Controller. No sensitive, privileged, or financial data shall be processed.

3. Categories of Data Subjects

Data subjects are limited to employees of participating law firms and corporate legal departments who respond to the survey.

4. Categories of Personal Data

Personal data is limited to name, title, business email address, and firm/organization name.

5. Obligations of the Processor

- Process data only on documented instructions from the Controller
- Ensure personnel confidentiality
- Implement appropriate technical and organizational security measures
- Assist the Controller in fulfilling data subject rights
- Support compliance with Articles 32 to 36 of the GDPR
- Delete or return all personal data at the end of processing
- Make available information to demonstrate compliance and allow audits

6. Sub-processors

Processor shall only engage sub-processors with prior written authorization from the Controller. A current list of sub-processors will be made available upon request.

7. International Transfers

Personal data shall not be transferred outside the EEA without appropriate safeguards as defined by GDPR Chapter V.

8. Security Measures

Processor shall maintain state-of-the-art security measures appropriate to the risk, including encryption in transit and at rest, access controls, logging, and regular security reviews.

9. Breach Notification

Processor shall notify the Controller without undue delay, and within 48 hours, after becoming aware of a personal data breach.

10. Governing Law and Jurisdiction

This DPA shall be governed by the laws of the Controller's principal place of business, unless otherwise agreed in writing.

Appendix B – Vendor Sub-Processor List

The following is a current list of third-party sub-processors engaged by LexFusion Intelligence for the purpose of delivering the GenAI Adoption Survey platform. All sub-processors are bound by contractual obligations consistent with GDPR Article 28 and are subject to appropriate data protection agreements.

Vendor	Service Provided	Hosting Region	Certifications
JotForm Inc.	Survey form hosting and response capture	AWS (multi-region)	SOC 2 Type II, ISO 27001, PCI-DSS
Microsoft Corporation	Application hosting (Azure), email (Graph API), monitoring	USA (Azure – East US 2)	SOC 1/2/3, ISO 27001, ISO 27017
MongoDB Inc.	Database (Atlas dedicated cluster)	USA (Azure – East US 2)	SOC 2 Type II, ISO 27001
Cloudflare, Inc.	Web application firewall (WAF), CDN, TLS termination	Global (Anycast CDN edge network)	SOC 2 Type II, ISO 27001
GitHub, Inc.	CI/CD automation (GitHub Actions)	USA (GitHub.com)	SOC 2 Type II, ISO 27001

Appendix C – Glossary

This glossary defines key terms used throughout the information security documentation for the GenAI Adoption Survey platform.

AES-256
Advanced Encryption Standard with 256-bit keys; used to encrypt data at rest. Widely considered a strong standard for confidentiality.

Azure Active Directory (AAD)
Microsoft's identity and access management platform. Used to secure login, enforce multifactor authentication (MFA), and manage user roles.

Azure Virtual Network and Private Endpoint
A mechanism to isolate traffic to cloud services like MongoDB Atlas, ensuring access is only allowed via internal network links rather than public IPs.

CMK (Customer-Managed Key)
An encryption key controlled by the organization rather than the cloud provider. Offers greater control over key lifecycle and access policies.

DPA (Data Processing Agreement)
A contractual agreement required under laws like the GDPR that governs how a third party processes personal data on behalf of a controller.

Express.js
A lightweight web application framework for Node.js. Used for building server-side logic and APIs.

GitHub Actions
CI/CD platform integrated into GitHub. Used for automating deployment and code scanning workflows.

JIT (Just-In-Time Access)
A security control granting temporary, time-limited access to sensitive systems only when necessary.

JOI and Mongoose
JavaScript-based libraries used for validating API requests (JOI) and modeling MongoDB documents (Mongoose). Help enforce strict data schemas.

RBAC (Role-Based Access Control)
A method for limiting system access based on a user's assigned roles and responsibilities.

TLS (Transport Layer Security)
A cryptographic protocol that ensures encrypted communication over the Internet. Required for HTTPS and secure WebSocket connections.

WAF (Web Application Firewall)
Protects web applications by filtering and monitoring incoming HTTP requests, defending against threats like SQL injection or XSS.

OAuth2 (Authorization Framework)
Industry-standard protocol for token-based authorization. Used by Microsoft Graph to securely delegate email-sending permissions.

MongoDB Atlas
A cloud-based managed database platform offering automatic backups, encryption, and access control over a virtual network.

Cloudflare
A global content delivery network and security provider. Used for DNS, TLS termination, and edge-based protections such as DDoS mitigation.

Microsoft Graph API
A RESTful API platform by Microsoft that enables secure programmatic access to Microsoft 365 services, including email sending.

Appendix D – References

- Microsoft Azure compliance & audit reports: Microsoft Service Trust Portal (Service Trust Portal / Azure SOC 2 Type II audit documentation)
  - Service Trust Portal (Audit Reports)
  - System and Organization Controls (SOC) 2 Type 2
- Microsoft Defender for Cloud
  - Microsoft Defender for Cloud documentation
- Microsoft Graph API
  - Microsoft Graph security API overview
- Cloudflare compliance hub (SOC 2 Type II, ISO 27001, PCI DSS, GDPR, etc.)
  - SOC 2 Type II Report Link
- Jotform Enterprise SOC 2 Type II Compliance and Security Documentation
  - SOC 2 Type II Announcement
  - Security Documentation
- MongoDB Atlas Private Endpoint with Azure
  - Learn About Private Endpoints in Atlas

Explainer

Generative AI is advancing faster than the market can separate signal from noise. To get a handle on real change—amid unreal hype—many clients began surveying their provider networks on GenAI's evolving role in legal service delivery. Individually rational, these efforts cause unintended consequences: high-volume variants of similar questions, contradictory signals, and survey fatigue that slows the collective conversation.

This initiative replaces fragmentation with a coordinated process that produces composite benchmarks available to the entire ecosystem. Mirrored instruments—surveying both providers and clients—make misalignment visible by surfacing the expectations gap. It is an ongoing program designed for longitudinal learning, using disciplined, behavior-grounded questions analyzed at scale to produce decision-ready insight.

The Survey Instruments and the Benefits of Collaboration

Our goal is to improve the quality of information while substantially reducing burden for all participants.

Clients and providers are invited to use the Provider Survey—a co-designed instrument reflecting consensus questions from more than 20 major law departments, refined with input from dozens of Am Law firms. We also invite law departments to complete our Client Survey, a mirrored counterpart that reveals alignment, or lack thereof, between clients and providers.

For clients:

- *Lower burden.* L.E.G.A.L. designs, administers, and manages the Provider Survey on the client's behalf—so clients receive provider client-facing responses as if they had run the survey themselves, but without the administrative overhead.
- *Stronger provider benchmarking.* Benchmark providers against your panel and against a broader market-wide dataset no single client can assemble independently.
- *Peer law department insight.* Through the Client Survey, gain visibility into how peer law departments are approaching GenAI—an otherwise inaccessible perspective.
- *Clearer diagnosis of misalignment.* As a neutral third party, L.E.G.A.L. can ask questions clients would not receive candid answers to directly; paired client/provider mirrors surface root causes, not just symptoms.
- *A shared point of reference.* Ground internal and external conversations in common benchmarks—shifting discussion from anecdote to evidence.

For providers:

- *Lower burden.* Answer core GenAI questions once, not separately for every client; responses persist and are prepopulated so updates are selective.
- *Client-by-client control.* Disclosure is never automatic; providers decide whether/when to release client-facing responses to each Requesting Client.
- *Peer and client benchmarking.* Participation entitles providers to composite insights into peer behavior and evolving client expectations—intelligence firms don't get from one-off client surveys.
- *A safe space for candor.* A neutral third party can collect perspectives providers can't share candidly in bilateral surveys, used only in de-identified/aggregate form.

Commented [LV1]: Confirm italics vs. bold for lead-ins in lists throughout this Explainer section

Commented [KD1R2]: LEFT IN ITALICS SINCE CONSISTENT THROUGHOUT ENTIRE SECTION

- *A shared point of reference.* Common benchmarks improve the quality of client conversations and support internal strategy.

This is structured, behavior-grounded intelligence work. Across both sides of the market, we reduce burden through coordination while improving informational value through disciplined questions, analysis, and reporting.

What We Measure (and What We Don't)

- *Organizing principle.* Our core concern is commercial impact. If GenAI isn't changing who does what, how work is allocated or priced, and what clients spend, it isn't changing the market—yet. We therefore prioritize commercial inflection points: new work, moved work, pricing shifts, realized savings, and changes to sourcing rubrics or fee structures.
- *Scope guardrails.* Commercial impact is a deliberate constraint that limits what we capture. We don't seek to inventory every experiment or back-office efficiency, nor do we intend to become a policy repository. Rather, where depth is warranted, we facilitate selective follow-up, including our Case Study Canvas.
- *Temporal framing.* Doing | Planning | Thinking: We anchor in observed outcomes (Doing), map funded near-term change (Planning), and elicit reasoned medium-term views (Thinking) to support longitudinal analysis and comparability.

What We Ask (and Why)

- *Prioritize structured questions.* Burden versus comprehensiveness is a largely unavoidable trade-off. Defaulting to structured questions (checkboxes, dropdowns) lowers burden and enables benchmarking. We also recognize that blank space implicitly asks for an answer even when a respondent has nothing useful to add. Limiting narrative questions reduces noise and invites clarity rather than creative writing.
- *Leaving room for clarifications.* All structured questions include an optional commentary box for respondents who want to challenge a question or caveat an answer. Structured questions are inherently constraining, and respondents retain the discretion to express themselves fully if they determine doing so will enrich the conversation.
- *With opportunity to request additional detail.* We prioritize minimal baseline burden, while enabling deeper follow-ons when warranted. Our objective is to limit labor-intensive exchanges to (i) the clients that want deeper detail and (ii) the providers prepared to engage on that topic. For example, instead of an open-ended narrative like "What is your GenAI strategy?," our Provider Survey asks whether a provider has a formal, shareable GenAI strategy; the subset of interested clients can then request the document from subset of providers positioned to share it.
- *Case Study Canvas for depth, selectively.* A follow-up tool for use cases. Where clients want more detail on high-signal use cases, our semi-structured canvas captures design, workflow, and measurable impact while ensuring the core survey does not turn into an essay exam.
- *Intentional use, not ambient AI.* We distinguish deliberate use of generative systems from background "AI-enhanced" features so that activity measures and maturity signals are not diluted. Ambient AI is becoming ubiquitous; if we measure it the same way, it will drown out deliberate decisions and discrete efforts the instruments are designed to capture.

- *Mirrored instruments to surface the expectations gap*. Clients and providers answer parallel questions to make alignment—and misalignment—visible and actionable. Our goal is to map the expectations gap so that we can begin to close it.
- *Clear lines on disclosure*. We ask questions everyone cares about, and candor is essential for benchmarks to mean anything. Confidentiality enables candor in an industry otherwise premised on perfection. Client Survey responses are used solely for de-identified, composite benchmarking. Provider Survey responses are split: (i) Client-facing Questions 1–5 may be shared in provider-attributed form with a specific Requesting Client only if the provider explicitly authorizes release to that client; (ii) Questions 6–16 are never shared in a provider-attributable form and are used only for de-identified and/or aggregated benchmarking outputs (including de-identified visualizations where thresholds are met).

How Participation Works

- *Distribution*. Clients send a unique link to law firms and ALSPs to register for the Provider Survey. Providers respond once; answers persist and can be updated. If already in the system, registration converts to a simple release request. Providers may also participate proactively to establish a baseline and access applicable benchmarking outputs—just as clients proactively respond to the Client Survey to gain access to those composite findings.
- *Permissioning*. Providers decide which clients receive their client-facing answers. All other responses are used only in de-identified and/or aggregated benchmarking.
- *What participants get back*. The composite report is modular, and access depends on participation.
  - Clients that complete only the Client Survey receive peer law department benchmarking (de-identified, program-wide).
  - Clients that request Provider Survey responses receive provider client-facing answers (where authorized) and provider benchmarking outputs, subject to minimum thresholds.
  - Clients that do both receive both sections.
  - Providers receive de-identified benchmarking outputs, but sections based on Provider Survey Questions 6–16 are available only if those questions are answered.

Follow-Ups, Events, and Ongoing Program

The market has solid tech maps and lists of use cases. We're currently missing commercial-impact data and interrogable, in-depth case studies. Commercial impact is at the center of our survey design. And the base survey instruments are also calibrated to surface candidates for case studies. In addition to clients selectively requesting that providers fill out our Case Study Canvas, we will conduct our own follow-ups where answers indicate further inquiry may elucidate insights of interest to the larger market.

Selected case studies will be featured in the composite report and associated events—all opt-in, of course.

Consent-Driven Disclosure and Safe Benchmarking

Confidentiality is sacrosanct. Participation is opt-in. Disclosure is always consent-driven.

- No third party sees an identified/attributable response unless the respondent explicitly agrees in writing. We do not assume consent; we require it.
- No client sees a provider's client-facing responses unless that provider authorizes disclosure to that specific client. Benchmark outputs are subject to minimum thresholds, and de-identified visualizations are provided only where participation supports safe de-identification.

- No one, including their providers, sees attributed client responses; client responses only feed into de-identified and composite benchmarking.
- Aggregation and de-identification are the defaults; insights are presented in de-identified and composite form unless expressly approved otherwise.
- Optional case studies follow a strict, multistep process, with off-the-record interviews and mutual written approval before any attributed publication.
- Our platform uses enterprise-grade infrastructure whose providers maintain independent assurance artifacts (including SOC 2 Type II and ISO 27001), with encryption in transit (TLS 1.2+) and encryption at rest (AES-256 where applicable).
- Raw data is accessible only to the core research team at LexFusion Intelligence.
- This is a nondisclosure-first environment—no resale, no repackaging.

For more, see the L.E.G.A.L. Nondisclosure Policy and our Security Documentation.

Contact and Support

For questions about participation, permissions, or the policy, contact the LexFusion Intelligence team at LFIntel@baretzbrunelle.com.

FAQ – L.E.G.A.L. GenAI Survey Initiative

At a Glance

What it is: L.E.G.A.L. is a permissioned market-intelligence system built to measure how GenAI is actually changing the economics of legal service delivery. It combines (i) permissioned, client-specific sharing of a limited subset of provider responses (only where the provider authorizes release) with (ii) de-identified or aggregated benchmarking used to produce composite insights.

What it focuses on: L.E.G.A.L. focuses on GenAI's commercial impact—who does the work, how work is allocated and priced, and where legal spend is moving.

What it is not: L.E.G.A.L. is not a generic survey, an experiment roundup, or a tool inventory. It's designed to replace fragmented one-off client questionnaires with a coordinated baseline that produces comparable benchmarks.

What's in the system: The system contains three instruments, each with a distinct job:

- Client Survey (demand-side expectations)
- Provider Survey (supply-side reality)
- Case Study Canvas (optional follow-up depth where there's real signal)

Time required (current pilot estimates):

- Client Survey: ~20 minutes
- Provider Survey: ~90 minutes (largely front-loaded; updates are selective)

Who should complete it: Submit one organization-level response per survey (often collaboratively), representing the organization's integrated assumptions and choices—not individual opinions.

How clients participate: Clients (a) complete the Client Survey and/or (b) request Provider Survey responses from their law firms and ALSPs. Doing both is recommended but not required.

How law firms/ALSPs participate: Providers complete the Provider Survey in response to a client request or voluntarily to establish a baseline; responses persist and are prepopulated for future requests.

How sharing works: Nothing is shared automatically. Only Provider Survey Questions 1–5 may be shared with a Requesting Client—and only with the provider's explicit, client-specific approval. All other Provider Survey responses (Questions 6–16) and all Client Survey responses are used only in de-identified and/or aggregated benchmarking (subject to minimum thresholds).

What you get back: All participants receive a composite market report—modular, based on participation level. Clients also receive provider responses to core questions (Questions 1–5) as if they had administered the survey themselves, as well as peer and provider benchmarking outputs that scale with provider response volume.

Cost: Participation is free for both clients and providers (the business model is built on aggregate insights, not selling individual responses).

Basics

1. What is the L.E.G.A.L. GenAI Survey Initiative?

Driven by a collaborative effort of leading law departments, the L.E.G.A.L. (Leaders Exploring Generative AI in Law) GenAI Survey Initiative is a permissioned market-intelligence system designed to measure how GenAI is actually changing the economics of legal service delivery.

Rather than collecting opinions, experiments, or technology inventories, L.E.G.A.L. focuses on commercial impact—how GenAI is affecting:

- Who does the work
- How work is allocated and priced
- Where legal spend is moving

L.E.G.A.L. replaces fragmented, duplicative client surveys with a single, coordinated framework, using mirrored surveys of clients and providers to surface expectation gaps and produce decision-grade benchmarks that no individual participant could generate alone.

In short, L.E.G.A.L. is not a generic market survey. It is shared infrastructure for honest, comparable insight about GenAI's real impact on the legal market.

2. Why is this effort necessary when there are already so many GenAI surveys?

Most client-initiated GenAI surveys are individually rational—and collectively inefficient.

Law departments send bespoke questionnaires to their providers to understand what is real. Providers respond—repeatedly—to overlapping, slightly different questions. The result is predictable: high burden, inconsistent answers, survey fatigue, and very little reusable intelligence.

L.E.G.A.L. exists to replace that fragmentation with coordination.

Instead of each client running its own survey, L.E.G.A.L. provides a shared, consensus-based instrument that providers can answer once, and then reuse, to produce market-wide benchmarks that no bilateral survey can deliver.

Equally important, L.E.G.A.L. surveys both sides of the market. By pairing mirrored Client Survey and Provider Survey instruments, the initiative makes expectation gaps visible—revealing where clients' assumptions about GenAI diverge from providers' actual capabilities and economics.

In short, L.E.G.A.L. does not add another survey to the pile. It is a collaborative effort to provide a coordinated replacement for existing, individual client surveys—to reduce burden while materially improving signal for everyone.

3. What is covered in the Client Survey, the Provider Survey, and the Case Study Canvas, respectively?

L.E.G.A.L. uses three complementary instruments, each designed for a distinct role in the intelligence system.

The Client Survey captures the demand-side perspective—how law departments are approaching GenAI from a commercial and sourcing standpoint. It focuses on expectations about how GenAI will affect

workflows, staffing, pricing, and legal spend, as well as how those expectations are shaping current decisions. The Client Survey is fully structured and contains no required narrative responses, to minimize burden and maximize comparability.

The Provider Survey captures the supply-side reality—how law firms and other providers are actually deploying GenAI in ways that affect service delivery economics. It covers adoption, governance, and use cases, with particular emphasis on assumptions about efficiency, pricing, margins, and client demand. A defined subset of responses (Provider Survey Questions 1–5) may be shared directly with specific Requesting Clients at the provider's discretion to replace individual client surveys. The remaining responses (Provider Survey Questions 6–16) are not disclosed to anyone, including clients, in an identifiable (firm-attributable) form. They are used only in de-identified and/or aggregated benchmarking outputs—specifically (i) client-specific benchmark reports provided to Requesting Clients (subject to minimum thresholds) and (ii) the composite market report shared with participants.

The Case Study Canvas is a selective follow-up tool, not a general survey. It allows clients and providers to go deeper on specific GenAI use cases where there is real signal—without turning the core surveys into a narrative exercise. This is where workflow detail, safeguards, and measurable outcomes are documented, by permission, on a case-by-case basis.

Together, the three instruments balance breadth, comparability, and depth:

- Structured surveys for benchmarking at scale
- Targeted case studies only where additional detail is commercially meaningful

4. What is not covered in the Client Survey, the Provider Survey, and the Case Study Canvas?

L.E.G.A.L. is intentionally scoped. Its organizing principle is commercial impact—how GenAI changes who does what, how work is allocated and priced, and where legal spend moves.

That focus means we do not attempt to capture everything that is interesting about GenAI. In particular, L.E.G.A.L. is not designed to be:

- A comprehensive inventory of tools, pilots, or internal experiments
- A policy or compliance repository
- A deep dive into GenAI issues outside legal service delivery economics

Many topics critically important to clients and providers are outside L.E.G.A.L.'s scope of purpose. For example:

- Substantive legal advice on enterprise GenAI (products, services, operations)
- Deep data security questionnaires that require cross-functional alignment well beyond clients' law departments

Excluding genuinely important topics is not a value judgment. It is a disciplined choice: better signal with less burden.

5. What are L.E.G.A.L. case studies?

L.E.G.A.L. case studies are optional, opt-in follow-ups designed to go deeper where survey results indicate real signal.

They are not required for participation and are not part of the core benchmarking instruments. Instead, case studies provide a structured way to explore specific GenAI use cases in more detail—such as workflow design, safeguards, and measurable commercial outcomes—when doing so would be informative.

Key characteristics include:

- **Explicit consent required.** Case studies are developed only with affirmative permissions from participating organizations.
- **Purpose-built depth.** They capture nuance and context that would be inappropriate to require—or standardize—across the full survey population.
- **Controlled use.** Case study insights may inform composite findings and, where permission is granted, be referenced in reports, briefings, or events. No attribution occurs without express approval.

The intent is to preserve discipline in the core surveys—keeping them structured, comparable, and low-burden—while still allowing deeper exploration where it is commercially meaningful.

In short: Benchmark broadly, then go deep selectively—by choice, not by default.

6. If it is free, how does L.E.G.A.L. make money?

L.E.G.A.L. is free to participants:

- Free to clients that complete the Client Survey and/or request Provider Survey responses
- Free to providers that complete the Provider Survey, including access to composite benchmarking outputs

But L.E.G.A.L. is not charity—though that would be ironic for an initiative that centers on commercial impact. L.E.G.A.L. is a commercial undertaking operated by LexFusion Intelligence (Baretz+Brunelle) to build a decision-grade view of how GenAI is actually affecting legal service delivery economics.

L.E.G.A.L. generates value—and supports monetization—through aggregate insights, not individual responses, specifically:

- Building the industry's most robust dataset on GenAI's commercial impact in legal
- Using de-identified, composite findings as the foundation for briefings, events, research, and advisory work (including capital advisory and market strategy)

What does *not* happen:

- We do not sell individual participant responses.
- We do not provide third parties with access to identifiable, organization-level data.

In short: Participation is free because the business model is built on permissioned, de-identified market intelligence at scale, not on charging participants or commercializing their individual answers.

Commented [LV2]: Confirm italics vs. bold for lead-ins (both bulleted and otherwise) throughout this FAQ section

Commented [KD2R2]: BOLDED

Participation

7. How long does the survey take?

Data thus far puts the timing as follows:

- Client Survey: approximately 20 minutes
- Provider Survey: approximately 90 minutes

These estimates will be refined as the dataset grows.

The time commitment is not driven by narrative writing. There is only one required narrative question across both surveys. Most of the time is spent on structured questions that require explicit *thinking*—particularly about GenAI's commercial impact and the attendant operating assumptions that inform decisions being made today.

For many organizations, L.E.G.A.L. will be the first time those assumptions are articulated clearly. That work is valuable—but it is not trivial.

Commented [LV3]: Here and throughout the rest of this section, we presume simply "L.E.G.A.L." vs. "the L.E.G.A.L. GenAI Survey Initiative" is OK, but please confirm

Commented [KD3R2]: OK IS AS

The effort required, however, is largely front-loaded:

- Responses persist and are prepopulated for future requests.
- Updates are needed only when facts or assumptions change.
- Subsequent interactions therefore require materially less time.

Importantly, L.E.G.A.L. reduces—rather than adds to—existing survey burden. Many one-off, client-authored GenAI surveys are narrative-heavy and, on their own, take longer than L.E.G.A.L. The aggregate time savings should prove substantial.

Participating Providers can further compound these time savings by redirecting clients that send bespoke GenAI surveys to utilize L.E.G.A.L. instead. This allows providers to release existing responses if they so choose, rather than repeatedly completing new questionnaires, while still meeting clients' information needs.

In short: L.E.G.A.L. requires real thinking once, then dramatically reduces repeat effort—producing better signal with less cumulative time investment.

8. Who should complete the survey?

Each survey is intended to be completed at the organization level, not by an individual acting solely in a personal capacity.

Accordingly, responses should be owned by stakeholders who are trusted to accurately convey the organization's GenAI strategy and operating assumptions—including how GenAI is expected to affect workflows, staffing, pricing, and economics over time.

In many organizations, completing the survey is a collaborative effort, drawing on input from leadership, innovation, operations, pricing, or knowledge teams. L.E.G.A.L. supports multiple contributors, but the final submission represents one consolidated, firm-wide or department-wide view.

The goal is not to capture every internal opinion but to reflect the integrated set of choices the organization is actually making—or is prepared to make—as GenAI adoption evolves.

9. Is there a way to save in-progress responses? Can multiple people collaborate on one response?

Yes and yes.

As explained below in greater detail, submitting saves in-progress responses. Submission alone does not release responses. Submission is required in order to enable collaboration.

Collaboration is both supported and encouraged. L.E.G.A.L. is designed to capture a unified, organization-level view, and many of the questions might benefit from input from more than one stakeholder.

While online collaboration is enabled, most collaboration will occur offline. All L.E.G.A.L. materials, including the annotated survey instruments, are available on the L.E.G.A.L. website for review or download, in both human- and machine-readable format.

Submitting vs Releasing Responses. At the bottom of each survey instrument, there is a single action button—*Submit*—which serves two purposes:

- It saves responses to the system.
- It makes the most recent version available to optional collaborators.

Submitting the survey saves your current responses to the system and enables collaboration. Submission alone does *not* release responses.

Release requires an independent authorization step—a separate Acknowledgment checkbox at the end of the survey. Release therefore depends on two conditions:

- Submitted survey responses
- Release authorization

Responses are released only if both conditions are met. For the Provider Survey, this means authorized client-facing responses are transmitted to the client at the close of the response period only if the client-specific release authorization is active.

Key points to note:

- You may submit and update the survey *without* authorizing release.
- Authorization may be withdrawn at any time, prospectively.
- In the case of the Provider Survey, authorization is client specific (i.e., granted on a client-by-client basis) and must be active when the response period closes in order for responses to be transmitted.

In short, submission controls saving and collaboration, whereas release authorization controls visibility.

Primary Point of Contact. The Primary Point of Contact serves as the organization's designated representative responsible for L.E.G.A.L. administration and communication.

Until the Primary Point of Contact is designated, the system defaults to the first email address to register for L.E.G.A.L.. The Primary Point of Contact may be designated, or changed, at any time at the top of the survey instrument. But there is only one Primary Point of Contact at any given time—for providers, it is not set per Requesting Client and does not change per submission. Thus, while organizations may designate any individual, we recommend using a group inbox, where feasible, for the Primary Point of Contact to ensure continuity.

Indeed, to avoid duplicate effort and keep one organization-level response, once an organization's L.E.G.A.L. profile exists, we route subsequent registrations from the same organization to the established Primary Point of Contact to connect colleagues internally and coordinate participation—e.g., by adding collaborators.

Optional Collaborators. Along with the Primary Point of Contact, organizations may list additional collaborators by providing their email addresses in a separate field at the top of each survey instrument. Collaborators are granted access to contribute to the organization's unified survey response. In the case of the Provider Survey, collaborators are client-specific—i.e., different collaborators are added to the form associated with a specific client and, unlike responses and the Primary Point of Contact, are not shared between forms.

While the system supports multiple contributors, it does *not* support simultaneous co-authoring—that is, per the above, responses must be submitted to be saved and made available to collaborators. Think of this like a document management system: Submitting the survey is equivalent to checking the document back in so others can work from the current version.

Thus, at any given time, only one person should be editing the survey. Other collaborators can continue work only after the current editor submits. This design preserves version integrity and prevents conflicting edits.

10. Do we need to submit more than one response? Can we?

No. L.E.G.A.L. accepts one unified set of responses per organization. However, responses are persistent and organizations can selectively update their responses over time.

The initiative is designed to operate at the organizational level, not the individual level. While organizations naturally contain differing views, L.E.G.A.L. is intended to capture the integrated position reflected in the organization's strategy and operating choices, not a collection of individual opinions.

Internal debate and collaboration are encouraged as part of arriving at consensus. But the final submission represents the organization's consolidated view at a specific point in time. Maintaining one official set of responses per organization is essential for comparability, benchmarking integrity, and longitudinal analysis—and for keeping L.E.G.A.L. decision-grade rather than anecdotal.

A potential supplementary use. Separately—and explicitly outside the current core L.E.G.A.L. benchmarking system—we are exploring a pared-down internal version of the commercial-assumptions portion of the survey. This would enable organizations to run an internal diagnostic to understand the distribution of beliefs within their own teams about GenAI's direction and speed of impact. Any such use would be optional, separate, and thoroughly explained when offered—to the point of likely having its own FAQ.

For Clients

11. How does L.E.G.A.L. benefit clients?

L.E.G.A.L. gives clients better intelligence with materially lower effort—at no cost.

Lower burden. L.E.G.A.L. operates the Provider Survey on clients' behalf, enabling clients to receive their providers' client-facing responses as if they had run the survey themselves—without the administrative overhead.

Stronger provider benchmarking. Clients receive benchmarked reporting that contextualizes their providers against a broader, market-wide data set that no single client could assemble independently—with client-specific panel views and richer diagnostics (e.g., distributions) delivered if minimum provider-response thresholds are met.

Peer law department insight. Through the Client Survey, participating organizations gain visibility (de-identified) into how peer law departments are approaching GenAI—another perspective that is otherwise inaccessible.

Clearer diagnosis of misalignment. As a neutral third party, L.E.G.A.L. can ask providers questions that clients would not receive candid answers to directly. When paired with mirrored Client Survey responses, this de-identified data helps surface the root causes of client–provider misalignment, rather than just its symptoms.

A shared point of reference. By grounding conversations in robust benchmarks made available to all participants, L.E.G.A.L. improves the quality of internal discussions and external provider dialogue—shifting conversations from anecdote and assertion to evidence.

12. How do clients participate in L.E.G.A.L.?

Clients participate in L.E.G.A.L. in two complementary ways.

First, clients complete the Client Survey, which captures their own expectations and assumptions about GenAI's commercial impact. This enables benchmarking against peer law departments and provides essential context for interpreting provider responses. Outside of the client's own internal use—i.e., comparing their answers to those of their peers and providers—Client Survey responses are used solely as de-identified/aggregated Benchmarking Data. Clients can register for the Client Survey on the L.E.G.A.L. homepage.

Second, clients request that their law firms and other legal service providers complete the Provider Survey. When a provider completes the survey, the client-facing portions of that provider's responses are shared with the Requesting Client as if the client had conducted the survey themselves, along with robust benchmarking that utilizes the de-identified responses and the global data set. This is a double opt-in process: Clients request responses, and providers decide whether to release them. Clients can register to send the Provider Survey to their law firms and ALSPs on the L.E.G.A.L. homepage.

Together, these two steps allow clients to see:

- How their own operations assumptions compare to peers
- How their providers compare with one another and the broader market
- Where, and how, their perspective differs from their providers (de-identified to enable candor)

What clients receive depends on how they participate (Client Survey only, provider requests only, or both). See the next question for the specific deliverables and the thresholds that unlock panel-level benchmarking and richer diagnostics.

13. Do clients need to take the Client Survey to request responses to the Provider Survey from their providers, and vice versa?

No. Clients may choose to do either, or both—but both is strongly recommended.

A client can:

- Only complete the Client Survey

- Only request Provider Survey responses from their providers
- Do both

Each instrument is valuable on its own:

- The Client Survey benchmarks your assumptions and decision posture against peer law departments.
- The Provider Survey benchmarks your providers against the broader market.
- But together, the mirrored instruments help pinpoint where misalignment originates—client expectations, provider realities, or both—so you can focus action where it will change outcomes (work allocation, pricing, controls, and spend).

What you receive depends on how you participate.

Complete the Client Survey only → peer composite benchmark report: You receive the de-identified, program-wide composite law department benchmarking shared with all participants. This lets you compare your own responses with the global results, internally.

Request Provider Survey responses only → provider responses and Benchmarks (where minimum thresholds met):

- Where you request Provider Survey responses and they authorize release to you (double opt-in), you receive providers' raw responses to Provider Survey Questions 1–5 just as if you had administered the survey yourself.
- Where you meet a minimum threshold of *five* providers releasing responses to you, you also receive:
  - Individual provider responses to Provider Survey Questions 2–4 benchmarked against both your provider panel's composite responses and the global provider data set
  - Your provider panel's composite responses to Provider Survey Questions 6–16 benchmarked against the global provider data set
- Where you meet a minimum threshold of *20* providers releasing responses to you, you also receive:
  - Individual provider responses to Provider Survey Questions 2–4 benchmarked against your provider panel's *segmented* responses and the *segmented* global provider data set
  - De-identified dot visualizations showing your provider panel's responses to Questions 6–16 benchmarked against the global provider data set

Do both (Client Survey + provider requests) → full client benchmarking (demand-side + supply-side), with richer diagnostics—you'll receive all the above, plus:

- Your responses benchmarked against the segmented global client data set and the global provider data set.
- Where you meet a minimum threshold of *five* providers releasing responses to you, you also receive your provider panel's responses benchmarked against your responses, the segmented global client data set, and the global provider data set.
- Where you meet a minimum threshold of *20* providers releasing responses to you, you also receive your provider panel's de-identified dot visualizations benchmarked against your responses, the segmented global client data set, and the global provider data set.

14. Do clients have to request responses from all their providers?

No. Clients have full discretion over which providers they include and how. Clients register to send the Provider Survey to their law firms and ALSPs on the L.E.G.A.L. homepage and then choose which providers to include. That said, peer law departments have already seeded the system with hundreds of requests. Thus, in practice, many requests to respond are automatically converted into release authorization requests—i.e., *Please authorize L.E.G.A.L. to send us the responses you've already completed and released to other clients.*

15. How do client requests to providers work in practice?

After clients register to send Provider Survey requests to their law firms and ALSPs on the L.E.G.A.L. homepage, we supply clients with ready-to-send outreach language containing a unique survey registration link that allows providers to register themselves. Upon registration, we take over administration, including follow-ups. If the provider already has a response on file, the registration process will surface this and convert a direct request (please complete the survey) into a release authorizations requests (please release your existing responses). Peer law departments have already seeded the system with hundreds of requests. Thus, many direct requests are automatically converted into release authorization requests.

16. Can clients ask their own questions? How does L.E.G.A.L. affect RFIs?

L.E.G.A.L. is a supplement, not a constraint. We expect clients to have, and ask, additional questions.

L.E.G.A.L. is a better way to collect, share, and benchmark the questions everyone is asking—not try to capture every question anyone is asking. The client-facing portion of the Provider Survey covers the common, core questions that providers are routinely asked across clients. As evinced in the many client-authored surveys we collected when creating L.E.G.A.L., these questions are being repeatedly answered in slightly different narrative forms. Providers answer these questions once in L.E.G.A.L. and update them only when facts or assumptions change.

This does not eliminate all RFIs; it allows RFIs to be narrower and more targeted. Rather than re-asking baseline questions, clients can focus RFIs on their specific requirements, risks, or use cases.

In practice:

- L.E.G.A.L. handles the shared baseline.
- RFIs handle what is truly bespoke.

The result is less burden for providers, better signal for clients, and cleaner separation between benchmarking and unique client needs.

Indeed, L.E.G.A.L. itself is premised on targeted follow-up. Not every common question is contained in the highly structured Provider Survey. Rather, the more narrative-heavy Case Study Canvas is the instrument designed for deeper dives. Instead of asking every question to every firm, we encourage clients to be selective in determining not only which providers but which specific use cases merit the effort required on both sides to engage constructively on the details of integrating GenAI into legal service delivery.

For Providers

17. How does L.E.G.A.L. benefit providers?

Just as clients get better intelligence with less effort, providers get fewer surveys, more control, and better insight without giving up confidentiality or negotiating leverage—at no cost.

Lower burden. Providers answer the core GenAI questions once, not separately for every client. Responses persist and are prepopulated for future requests, allowing providers to update only when facts or assumptions change rather than starting from scratch each time.

Client-by-client control. Disclosure of client-facing responses is never automatic. Providers decide, on a client-by-client basis, whether and when to release their responses. This preserves normal bilateral control while eliminating duplicative effort.

Peer and client benchmarking. Participation entitles providers to composite benchmarking insights, calibrated by participation level, showing how peers are approaching GenAI's commercial impact and how client expectations are evolving—intelligence providers do not receive with one-off, client-mandated surveys.

A safe space for candor. As a neutral third party, L.E.G.A.L. can ask questions providers could not answer candidly if clients saw the responses. These perspectives—presented only in de-identified form—allow providers to avoid commercial risk but still surface valid concerns about pricing pressure, mixed messages, and unrealistic expectations.

A shared point of reference. With both client and provider data in the system, L.E.G.A.L. creates a common factual baseline that improves the quality of conversations, both with clients and for internal strategic decision-making.

18. How do law firms and ALSPs participate in L.E.G.A.L.?

Law firms and ALSPs participate in L.E.G.A.L. by completing the Provider Survey.

Providers may complete the Provider Survey in response to a client request. This is the most common entry point and allows providers to respond once to a standardized set of questions that multiple clients can reuse—subject to the provider's client-specific authorization decisions.

Or providers may participate voluntarily, even absent a specific client request. Voluntary participation allows providers to establish a baseline and gain access to composite benchmarking insights.

In all cases:

- Providers submit one firm-wide response, not client-specific versions.
- Responses persist and are prepopulated for future requests, with updates made selectively only when facts or assumptions change.
- Client-facing sharing is entirely permission-based on an individual, client-by-client basis.

Participation is designed to minimize effort while maximizing reuse, control, and insight—both immediately and over time.

Once a provider participates in L.E.G.A.L., it is in their interest to encourage clients that send bespoke GenAI surveys to use L.E.G.A.L. instead. This allows the provider to release existing responses, if they so choose, rather than completing yet another one-off questionnaire, while still meeting the client's information needs.

19. Why would a provider participate voluntarily—i.e., absent a client request?

Voluntary participation is primarily about benchmarking and preparedness.

Benchmarking access. Participation is the mechanism by which providers receive the L.E.G.A.L. composite benchmarking report—calibrated to level of participation—including insight into peer behavior and evolving client expectations.

Establish a baseline before the first request. Completing the Provider Survey in advance also allows a provider to set a firm-wide, consistent baseline, rather than responding under time pressure when the first client request arrives.

Reduce future friction. Because responses are persistent and prepopulated, participating early means subsequent client requests require minimal incremental effort—update if needed, then decide whether to release client-facing responses.

Redirect duplicative client surveys. Once a provider participates in L.E.G.A.L., they can encourage clients that send bespoke GenAI surveys to use L.E.G.A.L. instead. This allows the provider to release existing responses, if they so choose, rather than completing yet another one-off questionnaire, while still meeting the client's information needs.

In short, providers participate voluntarily to gain market-grade insight, get ahead of inbound requests, and replace fragmented client surveys with a single, reusable source of truth—all while retaining full, client-by-client control over what is shared.

20. Are all the questions mandatory? Do firms need to respond to Questions 6–16 of the Provider Survey?

While no individual question is mandatory, clients will be made aware of missing responses, including Questions 6–16, while the composite benchmarking that is a benefit of participation is also calibrated to participation—i.e., providers receive benchmarking only for the questions in the survey in which they participated.

L.E.G.A.L. is designed to be transparent about what is and is not included in any given dataset:

- **Client-facing extract (Questions 1–5):** If a provider authorizes release to a Requesting Client, that client receives the provider's submitted responses to Questions 1–5 as if the client administered the survey directly. If a provider leaves an item blank, the client will see that it is unanswered.
- **Client-specific benchmark reporting (Questions 1–16; hybrid identified + de-identified):** Client-specific benchmark segments are shown only where at least five providers are included; de-identified dot plots/distributions are shown only where at least 20 providers are included. Where these minimum thresholds are met, client-specific benchmark reports may include dataset completeness transparency at two levels:
  - *Panel coverage list*: A list of firms included in the report (submitted + authorized release to that Requesting Client) and firms requested by the client but not included (did not submit and/or did not authorize release)
  - *Question-level completeness*: Within specific benchmarks, identification of which included firms are not included in that benchmark because they did not answer the relevant question(s).
- **Composite market reporting (program-wide):** In the composite market report, no providers (whether included or excluded) are identified without express permission.

In short, providers can skip any question, but nonresponse will be visible in client-specific reporting as "not answered" and/or through question-level completeness notes, while the benchmarking the provider receives will be limited to the questions in which they participated.

Optional is Truly Optional (Questions 17–24). The express exception to the above is the optional section. As the instructions state, "If a question sparks a strong answer, we'd love to hear it. If not, skip it." The optional section is the safe space for providers to enrich the collective conversation by selectively commenting on topics where they have strong opinions and supporting (anonymous) anecdotes. There will be no reporting whatsoever on which providers responded to which questions in the optional section. Indeed, absent express permission, we will not use verbatim quotes, even in a de-identified manner—we will only summarize and paraphrase.

Confidentiality, Sharing, Data Handling, and Security

21. How does controlled client-facing sharing work for providers?

Client-facing sharing is permission-based, client-specific, and never automatic. When a client requests a provider's responses, the provider decides whether and when to authorize release of responses to that specific Requesting Client. No responses are shared unless the provider explicitly authorizes disclosure to that Requesting Client.

L.E.G.A.L. uses provider responses in two distinct lanes, with different visibility rules.

Lane 1 – Controlled full disclosure (Provider Survey Questions 1–5)

What can be shared: Only Provider Survey Questions 1–5 are eligible for direct, provider-identified sharing with a Requesting Client.

When sharing happens: Responses are shared only when the provider has expressly authorized disclosure to that specific Requesting Client (client-by-client permission).

How it is treated: When released, responses are treated as confidential provider-to-client information, as if the client had administered the survey directly; this does not authorize sharing with other clients or third parties.

Fresh releases and control: If a client requests a fresh release, providers receive advance notice and an opportunity (not an obligation) to update—or to withdraw authorization for that Requesting Client.

Withdrawal: Providers can withdraw authorization for a particular client at any time; withdrawal applies prospectively and does not require program-level withdrawal.

Lane 2 – Benchmarking and reporting (client-specific + program-wide; hybrid identified + de-identified)

Client-specific benchmark reporting (Provider Survey Questions 1–16): Requesting Clients may also receive a client-specific benchmark report that contextualizes provider responses, subject to strict visibility limits:

- *Questions 1–5*: Where the provider has authorized disclosure to that Requesting Client, Questions 1–5 may be reflected in provider-attributed form (including comparative views) in the client-specific report.
- *Questions 6–16*: Provider responses are used only in de-identified and/or aggregated form. Individual provider responses are not disclosed in a provider-attributable way, though they may be reflected as unlabeled points in de-identified visualizations where thresholds are met.

Participation and dataset completeness transparency: Client-specific reports may include (i) a panel coverage list identifying firms included in the client's report and firms requested by the client but not included (did not submit and/or did not authorize release to that Requesting Client), and (ii) within specific benchmarks, identification of which included firms are not included in that benchmark because they did not answer the relevant question(s). This identifies coverage and nonresponse—not any firm's underlying non-client-facing answers.

Minimum thresholds: No client-specific segment (including averages) is shown unless at least five providers are included for that question/segment. De-identified dot plots/distributions are shown only when at least 20 providers are included for that question/segment. Below these thresholds, the attendant benchmarks and visualizations are not provided.

Program-wide composite market reporting: Provider responses may also be used in program-wide, de-identified and/or aggregated benchmarking and longitudinal analysis, including the composite market report shared with all participants. No firms (whether included or excluded) are identified in the composite market report absent express, written opt-in.

Client Survey responses are never shared in attributable form

Client Survey responses are used only as de-identified and/or aggregated Benchmarking Data and are never shared with providers or other third parties in client-attributable form.

Thus, for providers, the key features of the model include:

- *Client-by-client control.* Authorization is granted (or withheld) separately for each Requesting Client. Granting access to one client does not grant access to any other.
- *Normal bilateral treatment.* When shared, responses are treated as confidential provider-to-client information—exactly as if the client had administered the survey directly.
- *Defined scope.* Only Questions 1–5 are eligible for provider-identified disclosure. Questions 6–16 are never disclosed in a provider-attributable form.
- *Persistence with flexibility.* Once authorized, responses remain available to that client unless the provider chooses to update them or withdraw release authorization. Providers are notified before any fresh release and may revise responses or revoke authorization if desired.

In short, L.E.G.A.L. reduces duplication without changing control dynamics: Providers retain full discretion, clients receive consistent information, and benchmarking remains de-identified by default. For more information, see the L.E.G.A.L. Nondisclosure Policy.

22. How do updates or revisions to responses work?

Responses in L.E.G.A.L. are persistent, updatable, and under participant control.

L.E.G.A.L. is designed as an ongoing intelligence system, not a one-time survey. When an organization completes a survey, its responses are retained as a baseline and prepopulated for future requests. Participants may update their responses at any time, but they are never required to do so unless something has materially changed.

For providers that have already responded, in particular:

- When a client requests responses, providers receive advance notice and have an opportunity (but not an obligation) to revise their answers before any authorized release.
- If a provider is satisfied with its current responses, no action is required.
- Authorizations to share responses with a specific client remain in effect unless the provider chooses to withdraw or modify them.

This model reduces repeat burden while supporting longitudinal analysis—making it possible to see which assumptions hold, which change, and how quickly the market is actually moving.

In short, participants do the thinking once, update selectively, and retain control throughout.

23. How is participant data handled and secured?

L.E.G.A.L. is designed to be safe by default: de-identified by default, consent-driven disclosure, and strict use limitations. All participation in L.E.G.A.L. is governed by the L.E.G.A.L. Nondisclosure Policy.

What we collect (and what we don't):

- We collect survey responses (client and provider), a program Point of Contact for administration and notices, and designated internal collaborators.
- If a client supplies provider contact emails to facilitate outreach, we use them only to administer that survey cycle and then delete.
- We deliberately limit collection and retention of personally identifiable information to what's needed for program administration.
- We also process limited system access and security metadata (for example, authentication/session logs) solely to protect accounts and administer secure access; it is not used for benchmarking and is not shared in controlled disclosures.

How information is used (and not used):

- We do not sell individual participant data. Data is used only to (i) transmit authorized provider responses to requesting clients (Questions 1–5 only), (ii) produce de-identified/aggregated benchmarking and trend analysis, and (iii) support deeper, opt-in collaboration where separately consented.
- Contact information collected for L.E.G.A.L. is used only for L.E.G.A.L. administration and is not added to marketing lists or repurposed for unrelated outreach.
- Client-facing disclosures never include Point of Contact or other contact information, client-supplied outreach email lists, or system access/security metadata.

Security and access controls:

- We maintain strict internal controls, including limiting raw submission access to the core project team and storing contact information separately from composite outputs.
- Security controls include encryption in transit and at rest, role-based access control, SSO/MFA protections for admin access, and defined retention/deletion operations for systems and backups.
- For more, see L.E.G.A.L.'s security documentation.

Contact information retention and deletion:

- Provider/client Point of Contact information is retained solely for program administration (e.g., notices related to fresh releases or dashboard enablement) and is not shared with other participants or Requesting Clients.
- Client-supplied provider emails (if provided for outreach) are used only for that outreach and then deleted on the policy schedule after the response period closes; ongoing administration relies on provider-entered Point of Contacts.
- "Deletion" refers to contact records stored in L.E.G.A.L.-specific program systems; it does not require purging ordinary-course business communications (e.g., email threads) or enterprise backups maintained under standard practices.

Important scope note:

L.E.G.A.L. is not designed for privileged communications or matter-level content. We do not request sensitive personal data (including special-category data), government identification numbers, financial account numbers, or HR/personnel records, and participants should not provide such information in free-text fields.

For full details, see the L.E.G.A.L. Nondisclosure Policy.

Evolution of the Initiative

L.E.G.A.L. exists to solve fragmentation through collaboration. But collaboration requires coordination—coordination that has costs we've now collectively paid.

The final survey designs reduce burden (i.e., answer once, reuse), surface alignment gaps between clients and providers through mirrored questions, and center on commercial impact as the clearest measure of meaningful change. Third-party administration enables candor by keeping non-client-facing responses confined to de-identified and/or aggregated benchmarking outputs, while composite benchmarking returns value to all participants at no cost—through de-identification by default and consent-driven disclosure where attribution is permitted.

Where We Started

Law departments were already surveying their providers, often with overlapping or duplicative instruments. We began by aggregating more than 20 of these surveys—a cumulative exercise in every sense.

We removed redundancies and improved clarity, but the result remained too long, too narrative-heavy, and too demanding. Segmenting the instrument into *Quick*, *Full*, and *Case Study* variants helped only marginally; the burden was baked in.

To address it, we launched the *Survey on the Survey*, asking clients and providers alike to tell us what was necessary—and what could be cut. The exercise sparked invaluable conversations and surfaced insights from both sides of the client/provider divide.

What We Learned

- **Individually logical, collectively inefficient.** Each client's survey made sense on its own, but in aggregate they dulled the collective conversation.
- **Narrative overload invites noise.** Blank boxes beg to be filled, even when the respondent has little to add.
- **Data for data's sake.** Many clients were collecting information they didn't use—often because the answers lacked clarity or comparability.
- **Wasted effort at scale.** Both sides spent hours crafting and reviewing long responses short on actionable insight.
- **Unspoken assumptions.** Many of the underlying issues that merit discussion are rooted in divergent assumptions that drive divergent expectations and actions.
- **Candor constraints.** Some essential questions can't be asked directly by clients—or answered candidly by providers—without creating bilateral commercial risk; de-identified and/or aggregated benchmarking creates a safe lane for market-level candor.

How We Pivoted

We reframed the design around a single, clarifying question: "*How will this be used?*"

Rather than start with a long list of legacy questions, we worked backward from the answers that would truly inform dialogue between clients and providers.

The organizing principle remained money—commercial impact as the signal of real change. But our focus shifted from comprehensive consensus to streamlined, decision-ready benchmarking. We put an enormous amount of effort into each question in order to reduce burden, enhance comparability, and optimize information value.

- The **Client Survey** is now fully structured—checkboxes, dropdowns, and scales for comparability.
- The **Provider Survey** contains only one required narrative prompt—a concise reflection on commercially meaningful use cases, divided across three time horizons: Doing | Planning | Thinking.

Comprehensiveness still has its place. Optional narrative sections invite respondents to elaborate only where they have something substantive to contribute—isolating true signal instead of producing essay-length noise.

The surveys are also built for structured follow-up. High-signal responses, especially around GenAI use cases, can evolve into deeper exploration through the Case Study Canvas, a semi-structured tool for turning promising examples into tangible explorations of successful deployments.

The Updated Instruments

- **Provider Survey:** Structured, reusable, and built for comparability
- **Client Survey:** Mirrored counterpart highlighting alignment gaps and maturity differentials
- **Case Study Canvas:** Optional, semi-structured follow-up for high-signal use cases

Design Rules

- **Signal first:** Every question must earn its place.
- **Structure over sprawl:** Closed-ended items dominate.
- **Comparability by design:** Standardized scales and mirrored prompts.
- **Follow-on expected:** Surveys flag issues for targeted dialogue—not essays.

Clarifying De-Identification (Post-Launch)

Shortly after launch, we received excellent questions from participants about how de-identification works in practice—especially in the context of Provider Questions 6–16 and detailed benchmarking. Those questions led us to sharpen our language so it more clearly reflects the balance L.E.G.A.L. is designed to achieve: creating safe conditions for candor while still delivering the most useful, detailed benchmarking possible through de-identified and/or aggregated outputs.

Bottom Line

Better together. The collaborative redesign transforms an overloaded process into a disciplined, high-signal dialogue—minimizing both noise and the burden of extracting meaningful insight.