VENABLE LLP

Agentic AI Is Here—Legal, Compliance, and Governance Risks You Need to Know

February 23, 2026

Michael A. Signorelli, Rob Hartwell and Heather West

Agentic AI is quickly moving from experimentation to deployment. Much of the public conversation has focused on consumer-facing agents like shopping assistants and scheduling tools. Less visibly, companies and other organizations are integrating agentic systems into internal databases, workflow tools, coding exercises, financial systems, customer relationship platforms, consumer-facing recommendation engines and support tools, fraud prevention and security systems, and third-party services. These AI agents act in the marketplace: initiating transactions, triggering processes, coordinating vendors, and making decisions and learning at speed and scale.

Agentic AI does not arrive in a vacuum. Existing legal frameworks apply to their activity, be they consumer data privacy laws governing the collection and use of personal information or generally applicable civil rights, sectoral privacy laws, common law, or employment laws. As companies begin to incorporate more autonomous AI systems, keeping those requirements in mind is a key part of an AI compliance program.

What Is Agentic AI?

Agentic AI differs from more common AI tools like generative AI chatbots because it can work independently, seeking human input only when needed. Agentic AI tools can be set to a task and will work on their own to identify how to best complete that task, analyzing, designing, and completing specific objectives with little human input. Importantly, those agents can also learn and adapt over time, so that those tasks are completed more effectively in the future.

Agentic AI Is an Evolution, but Scale Matters

Organizations have long relied on automated systems. Algorithmic trading, recommendation engines, and fraud detection tools all operate with limited autonomy. Agentic AI fits squarely within this tradition.

However, there is no single framework governing "agentic AI" as a category. Instead, these systems operate within existing laws, depending on what they do, who they affect, and how they are deployed. Consumer protection, data privacy, cybersecurity, sector-specific regulations, contracts, and common

law all continue to adapt to this innovation.

Key Agentic AI Legal Issues You Should Be Evaluating

1. **Data management and privacy:** Agentic systems frequently use multiple datasets, combine information dynamically, and generate new inferences. While existing privacy frameworks still apply, managing compliance in environments that act continuously and adaptively creates novel operational issues. Controls around de-identification, sensitive data, and data hygiene are key to managing privacy risks.
2. **Vendor and supply chain risk:** Many agentic deployments rely on layered ecosystems of model providers, tool vendors, hosting platforms, and integration partners. Updates upstream can materially change agent behavior downstream. Contracts, audit rights, transparency obligations, and change-management processes matter more when a system's actions can evolve rapidly without direct modification by the customer.
3. **Oversight and risk mitigation:** Rolling out new agentic tools that make autonomous choices affecting customer behaviors should be rolled into existing impact assessment reviews to help mitigate potential discriminatory outcomes and other unintentional negative impacts. How that testing occurs, and what thresholds trigger additional action, will be vital to risk mitigation going forward.
4. **Security and risk infrastructure:** Agentic systems are designed to be integrated across sectors and businesses. Legal and compliance teams should ensure that agents are authenticated, actions they take are authorized, and activity is logged and subject to necessary security controls, and understand how effectively override and shutdown mechanisms operate.
5. **Identity, authority, and attribution:** Agents typically act "on behalf of" an entity. Questions about who is responsible for the agent's actions are key. If an agent initiates a transaction or makes representations, legal teams need clarity on how that authority is scoped, documented, and disclosed and who is liable when things go wrong.

A Confident, Practical Path Forward for Agentic AI Compliance

Agentic AI is expected to be a dominant topic in 2026, with entities large and small seeking to implement efficient and exciting technology. As agentic tools become embedded in core business functions, legal and compliance teams have a critical role to play in ensuring that autonomy is matched with control, speed with oversight, and new tools with commonsense compliance strategies.

If you have questions or concerns around security, privacy, and governance for agentic AI, please contact the authors or Venable's Technology and Innovation Group to learn how we can help you lead the AI-driven future.