dreamleap®

Checklist : 10 Essentials for Deploying AI Agents Responsibly in Commerce

This checklist helps businesses ensure their use of agentic AI aligns with legal, technical, and operational standards

☐ **1. Define your use case**	📌 What exactly should the agent do – and not do ? Only with a well-defined scope can risks be assessed and compliance ensured.
☐ **2. Clarify liability & ownership**	📌 Who is responsible if something goes wrong? Responsibility must stay with the organization – not with the AI system or the vendor.
☐ **3. Ensure user consent & control**	📌 Is there a consent layer before the agent triggers binding actions? Users must know they're interacting with AI – and have the option to confirm key steps.
☐ **4. Understand legal frameworks and regulations**	📌 Does the use case fall under the EU AI Act (e.g., high-risk category)? Even non-EU businesses may be affected – Swiss companies included.
☐ **5. Assess data sources and privacy risks**	📌 What data is being processed, and is it GDPR/compliant with local law? Especially with customer data, transparency and proper handling are crucial.
☐ **6. Communicate AI usage transparently**	📌 Do users clearly see when AI is acting – and when a human is involved? Transparency builds trust and prevents legal misunderstandings.
☐ **7. Enable logging and traceability**	📌 Are agent decisions tracked and stored securely? Logs are essential for audits, debugging, and accountability.
☐ **8. Use defined agent workflows**	📌 Does the agent operate within an approved process? Fully autonomous agents are still too unpredictable – workflow-based agents offer better control.
☐ **9. Choose your vendor carefully**	📌 Does the vendor support legal compliance, logging, and data governance? Many tools excel technically but fall short on regulatory readiness – ask the tough questions.
☐ **10. Empower teams and establish governance**	📌 Are roles, escalation paths, and training in place ? Agentic AI requires cross-functional oversight – from IT to legal to business owners