10 Questions Every Company Must Answer

Before Your AI Tools Become a Legal Liability

This checklist is designed for international companies, technology startups, and foreign investors operating in Costa Rica. A "No" or "Unsure" answer to any question below signals a potential legal exposure under Ley 8968 (Costa Rica's data protection law), the EU General Data Protection Regulation (GDPR), or emerging AI regulation frameworks. Book a free consultation with AEGIS to discuss your results.

1. **Do you use AI tools that collect or process personal data?**
   Any AI system touching personal data of Costa Rican residents (chatbots, analytics, HR tools, CRMs) triggers obligations under Ley 8968. This includes third-party SaaS tools your company licenses. ☐

2. **Have your AI systems been reviewed against Ley 8968?**
   Costa Rica's data protection authority (PRODHAB) actively enforces Ley 8968. A legal review identifies your exposure before regulators do — and before a breach forces the issue. ☐

3. **Does your Privacy Policy disclose your AI data practices?**
   Ley 8968 requires transparent disclosure of how personal data is collected, used, and processed — including by automated systems. Generic privacy policies don't satisfy this requirement. ☐

4. **Do you have explicit, informed consent for AI-processed data?**
   Consent under Ley 8968 must be specific, informed, and freely given. Pre-checked boxes, buried terms, and blanket consent clauses are insufficient and legally vulnerable. ☐

5. **Do your AI systems make automated decisions about individuals?**
   AI systems used in hiring, credit scoring, pricing, content moderation, or customer profiling carry heightened legal risk. EU GDPR Article 22 rights (and emerging CR equivalents) may apply. ☐

6. **Do you transfer personal data outside Costa Rica?**
   Sending data to foreign servers — including cloud AI APIs (OpenAI, Google, AWS) — constitutes an international transfer under Ley 8968 and requires specific legal safeguards and PRODHAB registration. ☐

7. **Have you assessed GDPR obligations for EU-facing operations?**
   GDPR applies to any company that offers goods/services to EU residents or monitors their behavior — regardless of where the company is based. Fines reach €20M or 4% of global annual revenue. ☐

8. **Do you have a Data Breach Response Plan?**
   Ley 8968 and GDPR require breach notification to authorities (and often affected individuals) within strict timeframes. Most companies have no documented response plan and are caught unprepared. ☐

9. **Have your vendor agreements been reviewed for AI/data liability?**
   Software, SaaS, and AI tool contracts routinely include clauses that transfer data liability to you — the customer. Off-the-shelf agreements are rarely compliant with Costa Rican or EU law. ☐

10. **Does your company have a designated Data Protection Officer?**
    Under GDPR, a DPO is legally mandatory for companies processing sensitive data at scale. Under Ley 8968, a responsible data custodian is ☐