AI Compliance Roadmap

AI compliance should not be built around formal documents alone, but around the actual use case: what function the AI system performs, what data it processes, who may be affected by its outputs, and what risks may arise for users, clients and the business. For an AI company, a basic compliance roadmap should combine the requirements of the EU AI Act, the GDPR and an internal risk assessment.

EU AI Act

☐ The company's role in relation to the AI system has been identified: provider, deployer, importer, distributor or product manufacturer.

☐ A preliminary classification of the AI system has been conducted: prohibited AI practice, high-risk AI system, AI system subject to transparency obligations or lower-risk AI.

☐ It has been checked whether the AI product is used in areas that may create increased regulatory risk, such as employment, education, finance, health, law enforcement or access to essential services.

☐ Basic AI disclosures have been prepared for users where they interact with an AI system or receive AI-generated outputs.

GDPR

☐ Data mapping has been conducted: what personal data is collected, from which sources, for what purposes, where it is stored and to whom it is disclosed.

☐ The legal basis for each key processing activity has been identified, including training, analytics, profiling or automated decision-making.

☐ The Privacy Policy, Data Processing Agreement, cookie / tracking disclosures and vendor data protection clauses have been prepared or updated.

☐ The need for a DPIA has been assessed, especially where the AI system processes sensitive data, conducts profiling or may significantly affect users.

Risk Assessment

☐ The key risks of the AI product have been described, including data protection, bias, hallucination, misuse, cybersecurity, consumer protection, contractual liability and sector-specific risks.

☐ Risk controls have been identified, such as human oversight, user warnings, access restrictions, logging, monitoring, content moderation or an escalation process.

☐ The limitations of the AI system, permitted use cases, prohibited use scenarios and user responsibilities have been documented.

☐ A process has been established for periodic review of AI risks after launch, model updates, changes in data flows or expansion into new markets.