WRITTEN BY

MARTINA GAVALEC
Partner
CMS Slovakia

AI STRATEGY & COMPLIANCE

Slovakia stands at an inflection point. As supply chains, capital and talent shift across Europe, the businesses that combine disciplined governance with swift adoption of AI are more likely to secure outsized gains in productivity, exports and competitiveness.

Digital transformation is no longer about isolated IT upgrades. It is about rewiring how value is created, decisions are made and risks are governed. AI, including today's fast maturing GenAI, has become the driving force. The question for Slovak boards is not "if" but "how": how to capture productivity, profitability and growth while staying squarely within evolving EU and Slovak regulatory frameworks.

INNOVATION AND RISK MANAGEMENT

Two pillars already shape digital operating models in Slovakia.

First, data protection. The GDPR sets the baseline for lawful, fair and transparent processing. Building or buying AI therefore starts with privacy by design, data minimization, and clear controller–processor allocations with vendors. Second, cybersecurity. The Slovak Cybersecurity Act, updated to align with the EU's NIS2 regime, requires risk management, incident reporting and supply-chain assurance for essential and important entities. As more manufacturers, utilities and digital service providers embed AI into operations, boards should treat model pipelines, data stores and MLOps (machine-learning operations) tooling as "information systems" subject to security measures, monitoring and testing.

The EU's horizontal platform rulebook also matters. The Digital Services Act (DSA) sets due diligence duties for online intermediaries and sharper transparency for recommender systems-touchpoints that must align with companies' AI governance and audit trails.
The EU AI Act now provides a risk based framework across the AI lifecycle. High risk systems require conformity assessment, quality data, logging, human oversight and post market monitoring; certain practices are banned and transparency rules apply to some general purpose and generative models.

Slovak companies must classify use cases, allocate roles and evidence compliance through technical documentation and quality management systems to build data governance that can pass a regulator's "show me" test.

FOUR LEVERS OF COMPLIANCE

Strategy. Leading Slovak business adopters are moving from pilots to portfolios: selecting AI use cases tied to Profit & Loss metrics. Pair each use case with a compliance stance from day one: define the lawful basis, assess fundamental rights impact, and decide what must remain on prem for trade secret or export control reasons. This "value plus verifiability" approach accelerates scaling without regulatory rework later.

Governance. Effective AI is disciplined AI. Establish an AI risk committee spanning legal, data protection, production and HR. Map industrial data assets and record data lineage; implement data-subject rights workflows that operate at model scale; and ensure the Data Protection Officer and cybersecurity teams can audit model training and inference logs. Align supplier governance with controller-processor contracts under Slovak law and the GDPR and extend third-party risk management to model hosts, prompt-management tools and foundation-model providers.

Architecture. Treat data platforms and MLOps as regulated infrastructure. Encryption, access controls, red-team testing, model versioning, bias and robustness evaluation, and rollback procedures are not "nice to haves". For firms in sectors covered by the Cybersecurity Act, include AI components in incident-response playbooks, with clear thresholds for notifying the National Security Authority.

Culture. Transformation succeeds when people trust the systems they use. Provide practical guidance on responsible use of GenAI, including handling of personal data and trade secrets, and publish an internal register of approved tools and models. Train product owners to set measurable success criteria and to maintain human-in-the-loop checkpoints. This builds confidence with employees, customers and regulators alike.

AI DUE DILLIGENCE

For procurement, refresh templates to allocate AI Act roles explicitly, mandate disclosure of training data provenance, require cybersecurity controls aligned to Slovak law, and embed audit rights.

In transactions, elevate AI and data to primary diligence streams, catalogue high risk use cases, test for GDPR compliance and lawful bases, verify security certifications against the Slovak Cybersecurity Act, and examine exposure to the AI Act's prohibited practices. Integration plans should budget for remediation of documentation, consent workflows and monitoring systems needed for day one compliance.

A SLOVAK ROADMAP

Inventory AI systems in use or in development, classify them under the AI Act (prohibited, high risk, transparency obligated, or minimal risk), and identify the companies' role for each. Where systems are high risk, initiate a gap analysis against conformity requirements and plan for a quality management system and post market monitoring.

Every company should confirm GDPR records of processing are current, and test incident detection and reporting against Slovak cybersecurity duties, including supply chain coverage for model and data providers. If businesses operate online intermediary services or rely heavily on platforms, it is important to align with DSA transparency and notice and action processes, especially where AI moderates or recommends content.

Lastly, it is also important to update licensing terms to address training on your data, output IP, hallucination remediation, security controls, audit support, and change control for model updates that could shift an application into "high risk" territory under the AI Act.

WHY THIS MATTERS NOW

AI offers immediate gains ranging from predictive maintenance on factory lines, to intelligent routing in logistics, or to automated triage in financial services. Yet the opportunity travels with accountability. GDPR, the Slovak Cybersecurity Act and the EU AI Act now form a coherent spine. If a company can explain the data, evidence internal controls and monitor their models, it can scale with digital confidence across the Single Market.

Start small but think systemically - prioritize use cases with measurable P&L impact and invest in governance and architecture that satisfy Slovak and EU rules by default. Done well, digital transformation powered by AI will not just make Slovak businesses more efficient-it will make them more resilient, more innovative and more competitive in the markets that matter.