Decoding Tomorrow: BLG Primer on AI Governance

What is an AI governance framework and why does your organization need one?

AI governance programs are crucial for organizations seeking to leverage the incredible potential of AI today while ensuring compliance with current and future regulations. The diverse risks linked with the use of AI, such as biased outcomes, and breach of confidentiality emphasize the need to address legal, reputational, and commercial concerns especially in the wake of recent regulatory developments in Europe and Canada. Organizations navigate this evolving landscape by integrating existing obligations, anticipating legal developments, and incorporating soft laws into their governance approach. The AI governance framework serves as a valuable asset, enabling organizations to future-proof operations, stay prepared for regulatory changes, and build resilience in AI deployment.

What are the key components of an AI governance program?

1) Governance

Accountability

Guiding Principles. A cross-functional team of the organization's key risk management, legal, and product development employees should formulate AI principles aligned with the organization's core values, forthcoming AI regulation, and relevant AI governance standards.

Oversight Structure. Organizations should designate an individual and/or committee tasked with enforcing its AI principles. This role, akin to that of a privacy officer and their team in the realm of privacy, should include individuals with expertise in risk and information management, as well as legal matters. Potential titles for roles within this oversight structure include Chief AI Officer, AI Governance Counsel, and AI Ethics Committee.

2) Mapping

Accountability, Safety

Organizations should identify each AI system they use and its purpose(s). During this process, organizations must prioritize AI systems with a potentially high impact on individuals, and document whether each identified AI system involves the processing of personal information and the jurisdiction in which reside the individuals affected by its use.

3) Risk Based Classification

Privacy and Security, Safety

Organizations should evaluate the risks linked to the AI systems they use, determine the scale of these risks and classify them appropriately. This involves scrutinizing potential evidence of harm to health and safety, as well as assessing the risk of adverse impacts on human rights. Additionally, organizations should ascertain if the AI systems are deployed in sectors recognized for their significant impact on individuals' lives, such as access to services, law enforcement, and education.

4) Evaluating and Mitigating Risks

Evaluation of AI Systems. Organizations should select approaches and metrics to evaluate AI systems, aiming to identify specific risks associated with their usage. For instance, organizations may assess whether an AI system may create biased outputs through fairness audits, and an AI's systems safety through robustness testing and metrics related to failure rates.

Risk Mitigation. Organizations should implement mitigation measures as a response to the identified risks and document any residual risks. Each organization should tailor its mitigation measures to its risk tolerance, its guiding AI principles, and its commercial objectives.

5) Develop organizational policies and procedures

Each of the governing principles set out by the organization should be put into action through the development of the relevant tools, procedures, and internal and external policies, such as a policy governing the use of generative AI, an algorithm impact assessment, and a public plain language AI notice.

6) Monitoring

Organizations must establish ongoing examinations of their AI system risk assessments, along with the constant review of developed policies and procedures. The implementation of these monitoring strategies is crucial to ensure that the AI governance framework can adapt to evolving risks, technologies, and industry practices.

With AI regulatoy requirement on the horizon, your organization, by taking proactive measures, positions itself to seamlessly decode these requirements, ensuring uninterrupted operations while unlocking the full potential of AI.

For more information please contact:

Frédéric Wilson
Counsel
514.954.2509
FWilson@blg.com

Simon Du Perron
Associate
514.954.2542
SDuperron@blg.com

Catherine Labasi-Sammartino
Associate
514.954.2555
CLabasiSammartino@blg.com

BLG
Borden Ladner Gervais