SPENCER WEST

CORPORATE AI GOVERNANCE

BACKGROUND

The adoption of Artificial Intelligence (AI) is accelerating across all sectors, offering significant opportunities for efficiency, insight, and innovation. However, alongside these benefits come complex legal, ethical, and operational risks – including around discrimination, privacy breaches, intellectual property infringement, corporate governance and management oversight, responsibility for decision making, and even potential liability for a failure to use AI where it would have been appropriate.

Without clear governance on the use of AI, organisations risk reputational damage, legal exposure, and diminished stakeholder trust. No matter what sector or size, all businesses should consider implementing robust policies and procedures concerning the use of AI, including training on the limitations and risks of different types of AI system. Central to this is being able to demonstrate that AI is being used transparently, responsibly, and in alignment with core principles of accountability, fairness, and human oversight.

This document explores the key issues to consider when building an 'AI governance programme' - by which we mean a set of processes, standards, policies, and ethical guidelines that an organisation can implement to direct, manage, and monitor its AI activities. By implenting such a programme, an organisation can ensure that AI systems are developed, deployed, and used in a responsible, ethical, safe, and legally compliant manner.

SPENCER WEST

1. GOVERNANCE AND STRUCTURE

'How is AI managed and who is responsible for what?'

- Executive sponsorship and definition of organisational posture and risk tolerance on AI
- Management Oversight
  - Nominated AI personnel and /or committee dependant on organisation size.
- Define cross-functional stakeholder roles and responsibilities (across IT; Legal; Product; Marketing etc.)
- Board reporting in line with organisational approach to risk management

2. AI MAPPING & INVENTORY

'What AI do we have and how it is used?'

- Compile and maintain an AI Inventory of all systems, including:
  - Function, use case, data types, owner, vendor, training sources, risk classification.
- Differentiate between development and use of AI
- Utilise and single source of truth and starting point for risk assessments

3. RISK ASSESSMENT

'How do we understand, measure and address the risks of an AI use case?'

- Mandatory risk assessment before deployment, including:
    - Legal risks: liability, data protection, IP infringement
    - Ethical risks: bias, discrimination, lack of transparency
    - Operational risks: hallucinations, system failure, lack of robustness
    - Strategic risks: reputational harm, regulatory enforcement, missed opportunities
    - Negligence risk for non-use: Consider scenarios where the absence of AI may constitute a failure of duty of care.
- Recommendation of appropriate risk mitigation measures, tailored and proportionate to the use case.
- Assigning ownership and follow through of risk mitigation.
- Utilisation and adaption, where possible, of existing risk assessment processes (e.g., DPIAs) to avoid duplication and overlap

4. POLICIES AND PROCESSES

'What rules and guidelines should our people follow when developing or using AI?'

- Organisational charter articulating key universal messages and principles
- Operational policy with detailed rules of the road
- Clear articulation of low risk 'safe harbors' to allow speedy adoption in areas with minimal concern
- Review and adaption of existing polices in related areas (e.g., privacy; confidentiality; acceptable use etc.)

5. TRAINING & COMPETENCE

'How do we ensure our people understand and engage with responsible use of AI?'

Mandatory training at management and operational level including:

- Accountability, and AI trends (including risk of liability from non-adoption).
- Safe use of AI, IP risks, data protection, ethical design, and red-flag scenarios.

Negligence and non-adoption

- Ensure managers understand the need to evaluate the reasonable use of AI to avoid inefficiencies or foreseeable errors.
- Where an AI solution is clearly beneficial and low-risk, failure to adopt it (e.g., in compliance, audit, fraud detection) must be justifiable.

6. VENDOR AND THIRD-PARTY MANAGEMENT

'What controls should we impose on the third parties who supply us with AI?'

- Supplier assessment questionnaires and risk classification.
- Review of suppliers for security, bias controls, IP policies, training data provenance, indemnity coverage, and compliance with applicable laws.
- Design and implementation of appropriate contractual safeguards, including AI Addenda, tailored and proportionate to supplier risk.

7. AUDIT AND ASSURANCE

'How do we test that our AI governance programme is being adopted and followed in practice?'

Monitoring and logging:

- Track usage of AI systems, including logs of prompts and outputs (especially in generative AI tools).

Incident escalation:

- Relying on existing risk management processes, ensure all AI-related incidents engage relevant management /AI committee, including:
    - Incorrect or biased outputs
    - Potential IP violations
    - Data breaches
- Review of AI governance programme by internal audit or assurance function.

8. REVIEW AND CONTINUOUS IMPROVEMENT

'How do we keep our programme fit for the future?'

Annual Review of the programme and its components by management or the AI Oversight Committee and ratification by the Board.

Trigger reviews if:

- AI-related incident or complaint arises
- New laws or ethical standards are introduced (e.g. UK AI White Paper, EU AI Act)
- Significant new AI tools are implemented

OUR EXPERTISE

Spencer West can support clients in the end-to-end design and implementation of a suitable AI governance programme, relative to the specific requirements of any business. Our advice is practical, and client focused with a suite of 'key principles led' services including:

- Risk assessments
- Training and workshops
- Policy drafting and implementation
- AI contract reviews
- Gap analysis assessments
- Monitoring plan and review timelines
- Boardroom advisory

SPENCER WEST

CONTACT US

Lisa McKinnon-Lower
Partner – Criminal Defence Litigation

T +44 (0)20 7925 8080
M +44 (0)7809 868439
E lisa.mckinnon-lower@spencer-west.com

Nabeel Osman
Partner – Legal Risk & Disputes

T +44 (020)7925 8080
M +44 (0)20 7376 655761
E nabeel.osman@spencer-west.com

James Clark
Partner – Data Protection, AI and Digital Regulation

T +44 (0)20 7925 8080
M +44 (0)735 008012
E james.clark@spencer-west.com

SPENCER WEST

Spencer West is a full-service international law firm with over 360 partners globally, in 20 jurisdictions. Known for its innovative, collaborative, and partner-led approach, Spencer West combines global reach with local expertise – delivering exceptional legal solutions across corporate, commercial, real estate, litigation, dispute resolution, and private client matters and supporting communities worldwide through grants from its Foundation. Founder funded and lawyer-led, Spencer West is built on trust, integrity, and a commitment to empowering lawyers to restore their positivity and enjoyment of the practice.

GLOBAL HEADQUARTERS:
Longbow House
20 Chiswell Street
London EC1Y 4TW

+44 (0)20 7925 8080
info@spencer-west.com
www.spencer-west.com

x.com/SpencerWestUK
linkedin.com/company/spencer-west