Strategic Data Governance: Moving Beyond Compliance – Data as a Strategic Trust Asset

5.0 | 7 Minutes

TECHNOLOGY

23 February 2026

By **Benjamin Shepherdson**

1. Executive Summary: The Board's New Mandate

Data is the lifeblood of the modern digital economy and is often cited as an organisation's most valuable asset. However, without rigorous governance, this asset becomes a profound liability.

For the Board, data privacy is no longer a "back-office" IT function or a regulatory checkbox. It is a top-tier governance priority that directly impacts operational resilience, reputation, and shareholder value. In a digital world, trust is the currency of growth, and data governance is the vault where that trust is kept secure.

With the convergence of aggressive global regulations and the rapid adoption of Artificial Intelligence (AI), the stakes have never been higher. This brief outlines how the Board must pivot from defensive compliance to strategic oversight, integrating data privacy into a broader **Data Governance Framework** to build trust and competitive advantage.

2. The Governance Landscape

The Board's oversight role has evolved. Courts, regulators, and investors increasingly view cybersecurity and data privacy failures as a breach of fiduciary duty.

- **The Regulatory Shift:** We have moved beyond the GDPR. Emerging laws across Asia have created a complex patchwork of compliance

store, risky to hold, and legally dangerous.

3. Strategic Framework: Linking Privacy to Data Governance

To exercise effective oversight, the Board must ensure that privacy is woven into the enterprise Data Governance Framework.

A. Privacy by Design (PbD)

The Board must champion a culture where privacy is proactive, not reactive. "Privacy by Design" means controls are embedded into the development of products and systems from the start, rather than bolted on later.

Board Checkpoint:
Major IT changes (migrations, new platforms) must be preceded by a risk assessment. When regulators ask, "Where is the Data Protection Impact Assessment (DPIA)?", they are effectively asking: "Did you think before you acted?".

Case Study: The Cost of Implicit Consent

Amazon (Luxembourg/EU): A record **€746 million** fine was imposed for data protection breaches. The core issue? "Non-compliance" with transparency obligations. Although Amazon declared what data they collected, they did not explicitly ask for consent to process it for targeted advertising.

Lesson: Transparency is not optional; implicit consent is a liability.

B. Data Minimisation and Lifecycle Management

A major risk is "dark data"—information collected "just in case" without a clear business purpose. This data is a liability with no Return on Investment (ROI).

The Principle: "Collect only what is needed, keep it only as long as necessary".

Board Checkpoint:
Liability is cumulative. Every record you keep past its "expiry date" is a potential lawsuit waiting to happen.

Case Study: The Consequence of Unlawful Processing

Enel Energia (Italy): The Italian Data Protection Authority fined this energy giant **€26.5 million**. The company used customer data unlawfully for telemarketing calls without appropriate consent.

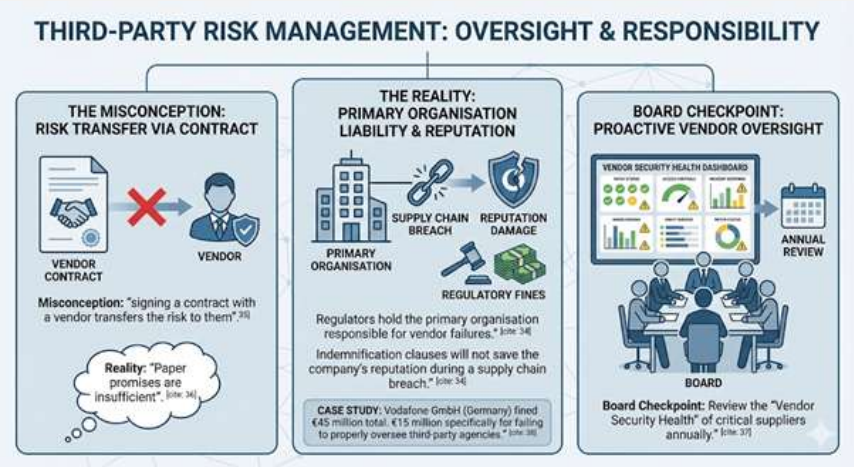
Lesson: Utilising customer data for purposes they did not agree to (secondary processing) triggers severe penalties.

Review the "Vendor Security Health" of critical suppliers annually.

Case Study: The Failure of Oversight

Vodafone GmbH (Germany): Fined a total of **€45 million** across two offenses. A **€15 million** fine was issued specifically for failing to properly oversee third-party agencies, which led to fraud. A separate **€30 million** fine addressed security deficiencies in their customer portal.

Lesson: You can outsource the work, but you cannot outsource the responsibility.

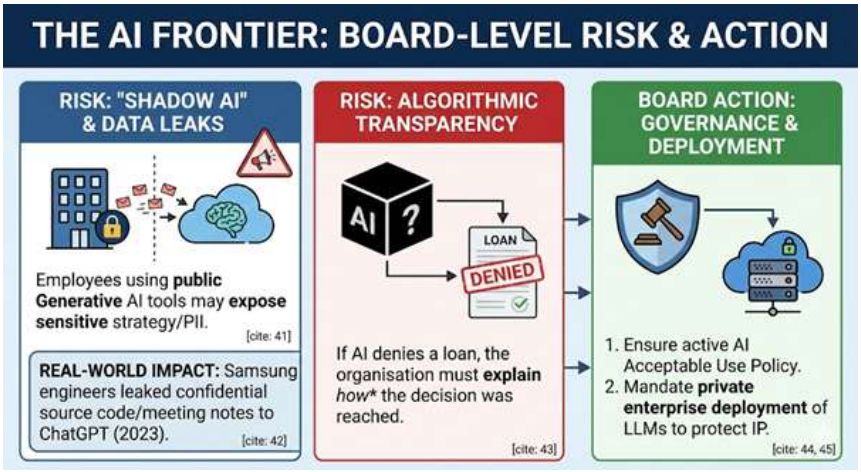


4. The AI Frontier: A New Dimension of Risk

The integration of Artificial Intelligence (AI) introduces complex challenges that require immediate Board attention.

- **"Shadow AI" & Leaks:** Employees using public Generative AI tools (e.g., ChatGPT) may inadvertently feed sensitive corporate strategy or Customer Personally identifiable Information (PII) into public models.
  - Real-World Impact: In 2023, Samsung engineers inadvertently leaked confidential source code and meeting notes to ChatGPT, exposing trade secrets to the public domain.
- **Algorithmic Transparency:** If an AI model makes a decision (e.g., loan denial) based on personal data, the organisation must be able to explain how that decision was reached.

Action:
Ensure an **AI Acceptable Use Policy** is active. Mandate the deployment of Large Language Models (LLMs) in the enterprise's own secure environment to protect intellectual property.



- What is our 'Crown Jewel' data, and where does it live?

Risk & Operations

- "Have we tested our Incident Response Plan in the last 6 months?" (Tabletop exercises are essential).
- What is our exposure to third-party data breaches?"
- "How are we managing the privacy risks of our AI initiatives?"
- "Do we have a 'Kill Switch' for our data flows?" (Can we isolate systems immediately?)

Resilience

- Are we prepared for the next wave of regulations?"
- "What is the status of our cyber/privacy insurance?"
- "How do we measure the effectiveness of our privacy training?" (Look for behavioural change, not just completion) .

6. Conclusion: The Path Forward

Data privacy is a journey, not a destination. Effective oversight requires a partnership where the Board sets the "tone from the top," emphasising that ethical data handling is non-negotiable.

Immediate Next Steps for ICDM Members:

1. Audit Board Skills: Ensure at least one director has technology/cyber competence. Tap into ICDM exclusive pool of visionary leaders. Refine your criteria and secure fresh mindsets while they build your robust talent pipeline.
2. Formalise Oversight: Assign clear data governance responsibility to the Audit or Risk Committee.
3. The Deep Dive: Dedicate one meeting annually solely to data strategy and cyber resilience.
4. Future-Proof Your Board: Join ICDM's globally benchmarked Director Programmes to equip your leaders with the tools to navigate tomorrow's challenges.

About the Author

Benjamin Shepherdson (MBA, CIPM, GRCP) is a seasoned governance and risk management leader with over 17 years of experience across high-stakes sectors, including Banking, Aviation, and Global Healthcare. Currently serving as a Data Protection Officer in the telecommunications sector. A member of the **Institute of Corporate Directors Malaysia (ICDM)**, Benjamin specialises in bridging the gap between technical regulatory compliance and strategic board-level oversight. He is widely recognised for his regional impact, having served as a trusted advisor to national regulators in **Indonesia**, **Thailand** and **Malaysia** to develop their official Data Protection Officer (DPO) competency frameworks.

Throughout his career—most notably leading the privacy strategy for **a Global Healthcare across 10 countries**—Benjamin has championed the concept of "Strategic Trust." He currently shares his expertise as an **Adjunct Lecturer at SMU Academy**, where he shapes the next generation of data governance professionals. Benjamin brings a unique "precision-under-pressure" perspective to corporate resilience, informed by his role as Deputy Chairman of Disaster Management for the **Malaysian Red Crescent Society**. He is dedicated to helping boards transform privacy from a regulatory hurdle into a primary driver of corporate integrity and sustainable growth.

The article was written by Benjamin Shepherdson.

Photo by Pavel Danilyuk on Pexels.com.

Artificial Intelligence (AI) | Enterprise Risk Management (ERM) | Technology Governance | Trust