AI, Data Protection, and Innovation: Getting Regulation and Best Practices Right

Key Takeaways

9 December 2024

AI, Data Protection, and Innovation: Getting Regulation and Best Practices Right

KEY TAKEAWAYS

9 December 2024

Dubai and Online

On 9th December, 2024, the Centre for Information Policy Leadership (CIPL) and the Dubai International Financial Centre (DIFC) Academy hosted an event on 'AI, Data Protection, and Innovation: Getting Regulation and Best Practices Right' in the margins of #RISK GCC Dubai. The event gathered experts for two discussions centered around key topics shaping the world of data policy and governance. Speakers included:

- Bojana Bellamy, President, CIPL
- Lori Baker, Vice President, Data Protection & Regulatory Compliance, DIFC
- Femi Daniel, Senior Counsel Privacy and Data Protection, Mastercard
- Francesca Gori, Regional Legal Lead – Asia Pacific, Middle East & Africa, Accenture
- Jelena De Lannoy, EMEA Privacy Officer, CISCO
- Kelly Tymburski, Senior TMT Legal Consultant & Managing Director, SPR Advisors FZ LLE
- Matthew Reisman, Director of Privacy and Data Policy, CIPL
- Ololade Shyllon, Head of Privacy Policy, Africa, Middle East and Turkey, Meta
- Renato Monteiro, VP – Privacy and Data Protection, e&
- Sarah Shaer, PhD Candidate, University of Chicago
- Tahir Latif, Global Practice Lead - Data Privacy and Responsible AI, Cognizant

Attendees represented a range of local and multinational companies, law firms, academics, and data protection regulators. Approximately 100 individuals attended the event, with 80 participating in-person and 20 joining virtually.

Below is a high-level summary of the key takeaways from the event.

DISCUSSION 1: TENSIONS AT THE CROSSROADS: EVOLVING DATA PROTECTION LAWS FOR AI

Key Points from the Discussion

- The Gulf Cooperation Council (GCC) region is rapidly growing and advancing compared to others, especially in AI. Bringing everyone together on the data protection front can be challenging, but AI could offer a valuable opportunity to foster collaboration and alignment. The DIFC has taken a unique approach to regulation of AI through Regulation 10, with a focus on “autonomous and semi-autonomous systems.”

- Some telecommunications companies are transforming into technology companies, with data and AI central to their operations. One telecommunications company shared that they

had over 400 AI use cases in 2024, and that they have established an AI Office and AI Committee that meet on a bi-weekly basis to assess these use cases throughout the year.

- Companies are placing AI at the core of their operations and are constantly researching new use-cases, such as how AI can address climate change, disease prevention and other societal challenges. This includes the development of innovative AI models. For instance, one company shared that they have recently created an AI model for high quality translations.

- Legal services are starting to use AI to improve efficiency but have experienced mixed results. It can help to identify relevant regulations but struggles to interpret laws in practice. Currently, it is still possible to identify contracts that have been generated by AI.

- Companies are still figuring out how to operationalise AI strategies. Their key focus areas should include: 1) Infrastructure: Large language models' workload requires 20 times more data centre bandwidth than traditional AI systems; 2) Cybersecurity: Data and models need to be protected from adversaries; and 3) Data Visibility: To determine which data can be used, it is essential to assess what the data is, why it is being collected, and how it can be used – if at all.

- Cisco's 2024 AI Readiness Index shows that 98% of respondents feel pressured to launch an AI project within the next 12 months, yet only 13% feel adequately prepared. There is a growing recognition of the critical requirements for success – governance, infrastructure, and talent. Despite this awareness, a disconnect remains between the ambitious goals organisations set and their ability to deliver on them.

- Global companies are working towards a unified AI approach while balancing differing international laws, which can be challenging. In the GCC region, companies are aligning with local laws based on the GDPR's principles, and are taking a best practices approach but are yet to face enforcement.

- Translating regulations into practice can be challenging, with regulatory fatigue affecting product teams, who have begun to question the need for compliance engineering over product features. Embedding compliance principles into the technology via "regulation" that formalises governance requirements is key for long-term success and building trust. In practice, this means creating a data scheme to categorise and tag data elements to understand what data is being collected and who it belongs to. It also requires intentional decisions about what data to retain, moving away from the tendency to hoard data "just in case".

- The GCC region is starting to recognise the value of data, with fewer restrictions on use compared to other jurisdictions. However, restrictions such as localisation still pose a compliance issue, especially as the localisation laws are not often enforced.

- Data protection laws in the region have some key differences from other jurisdictions. For example, the UAE lacks a "Legitimate Interest" provision, so companies are relying on global standards or establishing baselines for implementing regulations.

- One of the most important tasks for companies is figuring out where data originates, which is not always straightforward. There are two key considerations: 1) Identifying data sources and determining whether the data can be used; and 2) If new standards are introduced, establishing accountability instruments, such as risk assessments, to demonstrate compliance. Several companies stated that they use CIPL's Accountability Framework to ensure that they can demonstrate accountability and governance when needed.

- Product development moves faster than internal impact assessments. With regulations evolving rapidly, companies need risk-based frameworks to prioritise efforts. Regulators, such as the DIFC, want to learn from companies and understand their processes so they can support them. It can be challenging for companies to balance transparency requirements while protecting intellectual property.

- Privacy-Enhancing Technologies (PETs) can be used to assist regulatory compliance, especially for cross-border data transfers, and help maximise data use. Regulatory guidance, such as that provided by the Information Commissioner's Office (ICO) in the UK, is crucial in helping organisations understand how these technologies can support compliance efforts. However, it is important to remember that PETs are often use-case and industry-specific.

DISCUSSION 2: OPERATIONALISING EFFECTIVE AI GOVERNANCE

Key Points from the Discussion

- Research indicates that the most successful companies in AI are those that implement responsible AI practices, which foster trust and provide a competitive advantage. Responsible AI and governance are not just necessary, but fundamental to business success, with strong leadership from the board and C-suite being paramount.

- Employee training in AI is critical. One company shared that it employs multiple training methods for all employees on data strategy and responsible AI. It is essential for employees to have data literacy to understand how AI and data are used and to recognise their individual roles and responsibilities in this context. Engaging employees throughout the process is vital.

- One company has recently created a Chief Data and AI Officer role, distinct from the Chief Privacy Officer. While the Chief Privacy Officer focuses on compliance and legal interpretation, the Chief Data and AI Officer is responsible for evaluating AI use cases. These roles complement one another.

- Larger corporations can often more easily implement responsible AI standards due to their broader resources and teams. In contrast, talent and institutional infrastructure limitations can present significant challenges to AI governance for smaller organisations. SMEs, in particular, face difficulties in complying with these standards, as they are often under pressure to rapidly bring products to market.

- SMEs tend to allocate scarce talent and resources toward product development and services rather than compliance. Compliance should be driven by risk, and companies must assess where they stand on the risk spectrum in order to determine the appropriate compliance measures.