



Thought Leadership 2026

TDG:

Technology, Data, and Governance



Proof First, Scale Fast



Table of Contents

Foreword - From Trust to Proof	01
Executive Observation - From Rules to Proof Architectures	02
Acknowledgement	04
Editorial Advisory Team	05
Global Opening - Proof, Power and Scale: Governing Technology in a Polycentric World	06
Part I – Global Governance Anchors: China · the US · the UK	08
Mainland China - Building Scalable Data and AI Controls in Cross-Border Technology Business	08
Hong Kong SAR - From Principles to Proof: Building Robust and Reliable AI Governance	09
United States (California) - From Silicon Valley to Federal Scrutiny: Building AI, Data and Cybersecurity Governance Evidence	11
United States / United Kingdom - Whistleblowing, Data Protection, and Internal Controls as Evidence of Governance in Technology-Driven Companies	12
Part II – Europe	14
Opening Note - Proof Without Prescription	14

Switzerland - Open Finance as a Governance Laboratory: Switzerland's Market-Driven Path and PSD3/PSR	15
Germany - Observations on Contracting R&D on the Background of Global Knowledge Transfer	17
Germany - The Use of AI in Management and Supervisory Bodies: Finding the Right AI Governance Framework for Corporate Leadership	19
Hungary - Proof Before Prompt: Closing the AI Governance Gap in Hungarian SMEs	21
Poland - Proof Before Scale: Building an EU-Ready Compliance Architecture for China-Headquartered Technology Companies	23
Part III – Southeast Asia	25
Opening Note - Governing Scale Across Fast-Moving Digital Markets	25
Indonesia - Towards Responsible AI: A Governance Framework for the Digital Age	26
Malaysia - Technology Contracts That Scale: Managing Data, Intellectual Property and AI Risks in Cross-Border Collaborations	28
Malaysia - Considers Reforming Copyright Laws to Deal with AI Challenges	30
Cambodia - Trade Secrets as Technology Governance: Safeguarding Innovation and Investor Confidence in Cambodia's Digital Economy	32
Part IV – South Asia	34
Opening Note – At the Frontier of Digital Public Infrastructure: Operationalizing “Proof First, Scale Fast”	34
India - Cross-Border Data Governance in India: Making Digital Trust Scalable under the Digital Personal Data Protection Framework	36
Nepal - Governing AI and Data in Nepal Ahead of the Statute	38
Nepal - Emerging Markets - Aligning Cross-Border FinTech and Data Governance	40
Part V - Central Asia & Eurasia	42
Opening Note – From Digital Adoption to Proof-Based Governance	42
Uzbekistan - Digital Corporate Governance and Investor Confidence: Lessons in Uzbekistan	43
Kazakhstan / AIFC - From Sandbox to Proof Infrastructure: Making Digital Finance, Tokenised Assets and Cross-Border Investment Governable	45
Uzbekistan - Cross-Border Data Transfers under an Evolving Personal Data Legal Framework: A Jurisdictional Analysis of Uzbekistan	46

Uzbekistan - Building and Governing AI in Uzbekistan: Proving Data Compliance and IP Ownership Across the AI Lifecycle	48
--	----

Uzbekistan - Digital IP Protection: Protecting Software, Digital Content and Brands	50
---	----

Uzbekistan / Central Asia - Navigating Platform Liability and Cross-Border Data Governance in Emerging TravelTech Ecosystems: A Boardroom Playbook from Central Asia	52
--	----

Kyrgyzstan/Central Asia - Proving Cybersecurity Governance in International Commercial Arbitration: Digital Evidence as a Tool for Protecting Technology Investments	54
--	----

Turkey - The AI Shift in Arbitration: Efficiency Under Human Control	56
--	----

Turkey - Audit Trails Are Not Enough: Building Proof-Bound AI Decisions for Scale	58
---	----

Part VI - Africa	60
-------------------------	----

Sub-Saharan Africa - Governing the Digital Frontier: Data Protection, Cybersecurity and Responsible Technology Practice	60
---	----

Part VII- Latin America	62
--------------------------------	----

Opening Note - Latin America in a New Era of Cross-Border Governance	62
--	----

Brazil - Proving Governance in Brazil: A New Architecture for Technology, Data and AI	63
---	----

Chile - Chile's Compliance Runway: Open Finance, Cybersecurity and Data Protection as Governance Evidence	65
---	----

Mexico - Nearshoring Needs Proof: Data, Cybersecurity and Technology Governance for Mexico's Advanced-Manufacturing and Cloud Economy	66
---	----

Epilogue - Proof as the Condition for Scale	67
---	----



Foreword — From Trust to Proof

SLLS Global Thought Leadership 2026 is arranged as a four-part governance arc: ESS – CFI – TDG – TSR. Each edition examines a different stage of the cross-border business lifecycle. ESS asked how enterprise access remains credible through entry, scrutiny and stewardship. CFI asked how that credibility becomes bankable through capital, finance and infrastructure. TDG now turns to the systems that increasingly carry enterprise value itself: technology, data, artificial intelligence, intellectual property, cybersecurity and digital infrastructure. TSR will close the year by testing how those structures hold across trade, supply chains and resilience.

This Q3 edition is therefore not a general technology-law update. It asks a more practical question: when a company scales across borders, can it prove that its technology, data, AI systems, IP assets, digital platforms and governance arrangements are controlled, auditable, investable and capable of surviving scrutiny?

The method remains Rules – Rails – Results. Rules define obligations, permissions, restrictions and market-entry conditions. Rails are the operating mechanisms that carry those rules into practice: contracts, filings, data maps, technical controls, reporting lines, audit trails, board processes and dispute routes. Results show whether the structure works when regulators, investors, customers, counterparties or courts test it.

This edition also extends that method. In technology governance, rules change quickly, enforcement moves unevenly, and business models often scale before legal certainty arrives. Between rails and results, two further disciplines now matter: Records and Readiness. Records are the evidence that governance actually operated. Readiness is the capacity to respond when regulation changes, incidents occur, diligence begins or cross-border assumptions fail.

Across the jurisdictions in this volume, the details differ, but the operating question is consistent. Trust is no longer created by statements of compliance or innovation. It is built through proof that can be located, explained, tested and relied upon.

That is the practical ambition of this TDG edition: to help companies scale faster because they have first made their governance visible.

Steve Shi

SLLS Global

Executive Observation - From Rules to Proof Architectures



The most important movement across this TDG edition is not simply that technology regulation is becoming more detailed. It is that governance can no longer be credibly reconstructed after the fact. Across jurisdictions, companies are increasingly expected to show how their technology, data, AI systems, intellectual property, cybersecurity controls and reporting structures actually operated while business models were changing.

Compared with last year's TDG edition, the centre of gravity has shifted. The 2025 edition examined how digital trust could be engineered through Rules – Rails – Results: stablecoin reserves, tokenised securities, data-transfer gateways, industrial IoT evidence lockers, XR consent architecture, biometric safeguards and supply-chain provenance. That method remains valid. What has changed in 2026 is the pressure placed on the enterprise itself. The question is no longer only whether trusted rails exist in the market, but whether a company can produce its own records, controls and decision history when regulators, investors, customers, courts or counter-parties ask.

The global picture is increasingly polycentric, but several governance models are becoming visible. China demonstrates a pathway-based model in which data classification, export routes, personal-information audits, network-data risk assessments and AI labelling generate specific forms of evidence. The United States illustrates a layered model in which state privacy law, frontier-AI rules, federal standards, consumer-protection enforcement, securities disclosure and litigation combine to create accountability through multiple channels. Europe shows both prescription and discretion: Switzerland relies heavily on principles-based responsibility and institutional governance; Germany places AI directly within management and supervisory-board duties; Poland demonstrates how EU market access increasingly depends on connecting regulatory responsibility with the technical teams and records that actually hold the facts.

The same shift is visible outside the largest regulatory markets. India and Nepal show different ways of governing where statutory frameworks remain incomplete or transitional. Southeast Asia links AI governance, technology contracts, copyright and trade secrets to transaction readiness and investor confidence. Kazakhstan's AIFC illustrates how regulatory sandboxes, licensing, data infrastructure and dispute mechanisms can become institutional proof infrastructure. Uzbekistan shows how corporate governance, data transfers, AI, digital IP and platforms are converging around demonstrable controls. Türkiye adds a further insight: system-level audit trails may show that something happened, but consequential AI decisions increasingly require evidence of why an outcome occurred, which rules and model versions applied, and who had authority to act.

Latin America and Africa reinforce the same direction through different institutional paths. Brazil is strengthening enforcement capacity across data protection, child online safety and AI governance; Chile is using an implementation runway to connect open finance, cybersecurity and privacy controls; Mexico shows how near-shoring brings cloud, industrial data and IT/OT governance into the same operating environment. South Africa illustrates how data protection, cybersecurity, AI governance and board responsibility increasingly intersect rather than remain separate compliance functions.

Across these regions, the movement is therefore consistent even where the rules are not. Regulation is shifting from permission to evidence; from compliance statements to operating records; from isolated legal require-

ments to connected governance systems; and from local obligations to proof that must travel across borders. The recurring artefacts are strikingly similar: data maps, AI registers, consent logs, model and version records, vendor files, cyber incident records, board minutes, human-review checkpoints, contractual controls, whistleblowing channels and dispute-readiness mechanisms.

This is why the SLLS method now needs an extension rather than a replacement. Rules – Rails – Results still explains the movement from obligation to mechanism to outcome. TDG 2026 shows, however, that two additional disciplines increasingly determine whether that movement can be trusted: Records and Readiness.

The more mature formulation is therefore Rules – Rails – Records – Readiness – Results. Rules define obligations and boundaries. Rails translate them into systems, contracts, workflows, permissions and escalation channels. Records preserve evidence that those rails actually operated. Readiness tests whether the organisation can respond when regulation shifts, systems fail, incidents occur, diligence begins or disputes arise. Results show whether the structure remains investable, auditable, enforceable and scalable under pressure.

The practical conclusion is narrow but demanding. The companies best positioned for the next phase of cross-border growth will not be those that merely claim to be innovative, compliant or global. They will be those that can locate evidence, explain decisions, correct failures and adapt without losing control. In the next phase of technology governance, scale will belong to enterprises that can prove how they are governed.



Acknowledgement



SLLS Global gratefully acknowledges the authors, regional advisers, reviewers and supporting colleagues who made this Q3 TDG edition possible.

This volume reflects a genuinely cross-jurisdictional effort. Contributions were developed by legal practitioners, academics, institutional voices and business-facing experts across Asia, Europe, Africa, North America, Latin America. Their work brings together local legal knowledge, practical governance experience and international commercial perspective on technology, data, AI, intellectual property, cybersecurity, digital assets and cross-border operations.

We are especially grateful to the regional advisory contributors who supported this edition through topic shaping, contributor outreach, regional framing and editorial coordination. Their role helped ensure that the publication remained internationally readable while preserving the specificity of each jurisdiction.

SLLS Global also thanks the authors for preparing, revising and confirming their contributions within a demanding publication timeline. The purpose of this edition is not to produce a uniform view, but to present disciplined, practical and evidence-based perspectives on how governance is being built, tested and proven across different markets.

All contributions remain subject to SLLS Global's editorial standards of independence, accuracy, neutrality and practical usefulness.



Editorial Advisory Team

The SLLS Global Thought Leadership Series is developed through an editor-led process supported by selected regional advisers and specialist contributors. The Editorial Advisory Team assists with regional framing, contributor outreach, topic positioning and publication coherence. Final editorial responsibility remains with SLLS Global.



Steve Shi

Founder, SLLS Global

Email: steve@slls.global



Peter Ruggle

Attorney at Law, Founding Partner, RUGGLE PARTNER, Switzerland, Europe

Email: peter.ruggle@rugglepartner.ch



Dr. Kamola Batirova

Assistant Professor, Tashkent Metropolitan University, Central Asia and Eurasia

Email: batirovakamola@gmail.com



Upendra Raj Dulal

Partner / Advocate, Agrani Law Associates, Nepal, South Asia;

Email: dulalupendra@yahoo.com



Nicolene Schoeman-Louw

Founder and Managing Director, SchoemanLaw Inc · South Africa, Africa

Email: nf.schoeman@schoemanlaw.co.za



Dr. Tivadar Krisztián

Head of Office, Tivadar Law Firm, Hungary

Email: drtivadar@drtivadar.hu

Global Opening - Proof, Power and Scale: Governing Technology in a Polycentric World



Sector Focus: Strategic Autonomy · Proof Architectures · Technology Governance · Cross-Border Scale

Technology governance is becoming part of economic security and corporate strategy rather than a function applied after innovation. In a polycentric international order, the ability to demonstrate control over technology, data, AI, intellectual property and critical dependencies increasingly determines whether growth can travel across markets.

Technology now sits inside strategic competition. Governments intervene not only after products reach the market, but in data provenance, supply chains, sensitive-technology end use, investment ownership and infrastructure location. In Europe, the Data Act has applied since 12 September 2025, while the AI Act entered its general application phase on 2 August 2026, subject to subsequent recalibration of key high-risk-system timelines. Regulation (EU) 2026/1386 further strengthens foreign-investment screening, requiring Member States to operate national screening mechanisms when it becomes applicable from 17 January 2028. In the United States, controls on advanced semiconductors, computing capacity and chip-manufacturing equipment similarly make end users, destinations and diversion risks part of commercial governance.

The resulting environment is not deglobalisation so much as the politicisation of interdependence. Companies still operate across borders, but no longer within an assumed path toward regulatory convergence. A product may be technically viable yet constrained by data-provenance rules; an ownership structure may attract capital while triggering investment review; cloud infrastructure may improve efficiency but conflict with localisation, security or continuity requirements.

Formal compliance therefore answers only part of the problem. Strategic capacity means knowing which functions cannot be interrupted, which suppliers cannot be readily replaced, which data cannot move freely, which technologies face restrictions and which decisions must remain under the company's control. Strategic autonomy is not self-sufficiency; it is the ability to understand dependencies and retain decision-making capacity when one becomes critical.

That capability depends on a coherent proof architecture: an up-to-date inventory of technology and AI systems; evidence of data provenance and lawful use; clear allocation of responsibility; testing, impact assessments, decision logs and meaningful human oversight; visibility into cloud, chip, software, model and open-source dependencies; and incident procedures that preserve records and explain subsequent decisions. Frameworks such as NIST AI RMF 1.0, ISO/IEC 42001 and the OECD Due Diligence Guidance for Responsible AI can provide useful organisational structures, but only when translated into controls appropriate to the company itself.

Boards and investors should therefore ask whether critical systems are visible, intangible assets can be shown to be owned or lawfully used, authority to modify or suspend systems is clear, important decisions can be reconstructed, strategic dependencies are understood, geopolitical exposure is mapped and claims made to investors, regulators and customers are supported by available evidence.

Cross-border scale will increasingly require interoperability without uniformity. Companies need a common global core for responsibilities, security, system classification and incident response, combined with modular local arrangements for data transfers, impact assessments, user information, contracts and human oversight. The advantage lies not in eliminating regulatory difference, but in preserving organisational coherence while adapting to it.

Proof is therefore more than documentation prepared before growth. It is the infrastructure that allows growth to remain controllable, investable and transferable when technology, regulation and geopolitical conditions change.



About the Author

Tiberio Graziani

Chairman, Vision & Global Trends

International Institute for Global Analyses

Tiberio Graziani leads Vision & Global Trends, the International Institute for Global Analyses. His contribution focuses on the relationship between technology governance, strategic autonomy, geopolitical interdependence and the institutional conditions required for cross-border growth.

Email: tibgraziani@gmail.com



Part I - Global Governance Anchors: China · the US · the UK

Mainland China - Building Scalable Data and AI Controls in Cross-Border Technology Business



Sector Focus: Cross-Border Data · AI Governance · Cybersecurity · Governance Evidence

China's technology-governance framework is moving beyond the narrow question of whether data may leave the country. For companies operating across China and overseas markets, the more demanding question is whether they can demonstrate what data they hold, how it is classified, why a transfer is necessary, which legal route applies, who receives the data, and what controls continue afterwards. The same evidentiary logic increasingly applies to AI systems, where training-data provenance, labelling, personal information handling, human review, vendor controls and incident response form part of the governance record.

The 2024 Provisions on Promoting and Regulating Cross-Border Data Flows clarified the distinction between lower-risk transfers and those requiring formal mechanisms. Certain transfers may be exempt where no personal information or important data is involved, while non-CIIO processors exporting personal information involving fewer than 100,000 individuals, excluding sensitive personal information, may also qualify for exemptions. Higher-risk transfers remain subject to security assessment, including exports of important data, personal information involving at least 1 million individuals, or sensitive personal information involving at least 10,000 individuals. Selecting the correct route therefore depends on understanding the data, business purpose, processor status and applicable sector rules.

"Important data" requires disciplined classification rather than assumption. Where data has not been identified or notified as important by relevant authorities or regions, companies need not treat it as important for export-security assessment purposes. By March 2025, 298 data-export security assessment projects had been completed; 44 involved important data, seven were not approved, and 325 of 509 declared important-data items were permitted to leave China after assessment. The issue is therefore whether a transfer can be justified and controlled, not whether important data is automatically immovable.

Governance is also becoming continuous. The Network Data Security Management Regulations took effect on 1 January 2025, followed by the Personal Information Protection Compliance Audit Measures on 1 May 2025 and the Network Data Security Risk Assessment Measures on 20 August 2026. AI governance follows the same direction through generative AI rules, algorithm filing requirements and the AI-generated content labelling regime effective from 1 September 2025.

For cross-border businesses, the practical response is an evidence architecture rather than a filing archive: data maps, classification records, transfer-decision memos, impact assessments, vendor controls, AI use-case registers, training-data provenance records, incident logs and management dashboards. These materials support regulatory review, customer audits, investor diligence and post-incident accountability. Scale becomes defensible when higher-risk data and AI activities can be identified, governed and evidenced without breaking the wider business.

About the Author

SLLS Global Research Team

Hong Kong SAR - From Principles to Proof: Building Robust and Reliable AI Governance



Sector Focus: AI Governance · Risk Classification · Third-Party AI · Data & IP · Transaction Readiness

Hong Kong's AI governance model is developing through existing legal regimes, sectoral supervision and non-binding guidance rather than a standalone AI statute. For companies, that flexibility increases the importance of being able to show how AI systems are classified, approved, monitored and controlled in practice.

Hong Kong's Ethical Artificial Intelligence Framework ("Ethical AI Framework"), Generative Artificial Intelligence Technical and Application Guideline ("Generative AI Guideline") and 2026 "Trusted AI in Practice" materials collectively point toward a governance model built around risk classification, accountability and evidence. The Ethical AI Framework uses a three-lines-of-defence structure: project teams manage design and initial risk mitigation; steering and assurance functions provide independent review; and senior technology or governance leadership provides continuing oversight. Rather than creating a standalone AI committee, companies may embed AI responsibility into existing risk, audit, technology or conduct structures, supported by a clearly identified senior executive owner.

The Generative AI Guideline adds a four-tier classification covering unacceptable, high, limited and low-risk uses. Translating that structure into internal governance requires companies to define risk criteria relevant to their own business, maintain a register of material AI systems and reassess use cases when data sources, model autonomy or deployment scope changes. High-risk AI use cases-such as credit scoring, trading algorithms or systems with material legal consequences-may require explicit approval, meaningful human over-

sight and closer monitoring.

Auditability is central. Companies should be able to produce an inventory showing where AI is used and who owns each system, data-lineage and training-data records, model version and change logs, and evidence of human review or override in higher-risk contexts. For agentic AI and copilots, logging should be proportionate enough to reconstruct significant decisions without creating unnecessary data accumulation. Procedures should also allow systems to be suspended, disabled or rolled back where incidents occur.

Third-party dependency is another significant governance issue. AI capabilities increasingly rely on cloud infrastructure, foundation models, APIs and external vendors. Boards and management therefore need visibility over model ownership, hosting locations, data-use rights, security standards, model changes, rollback arrangements and termination consequences. Contracts should address ownership of fine-tuned models and outputs, the provider's right to use customer data, security obligations and notification of material model changes.

These controls increasingly matter in transactions. Claims about "proprietary AI", accuracy, efficiency or fairness may appear in fundraising materials, M&A documentation and pre-IPO disclosures. Investors and advisers may therefore ask whether those claims are substantiated, whether training data and outputs can lawfully be used, what incidents have occurred and what governance documentation exists. AI-related warranties, covenants and post-closing remediation may follow where gaps are identified.

A practical AI governance pack can bring the evidence together: governance policy, system inventory, risk classifications, human-oversight controls, third-party safeguards, incident logs and board reporting. Hong Kong's guidance-led model gives companies room to design governance proportionately, but that discretion comes with a corresponding burden: the organisation must be able to explain and evidence why its AI use and controls are reliable and credible.

About the Author

Sam Wu

Partner, YYC Legal LLP · Hong Kong

Sam Wu is a Hong Kong solicitor with over 10 years of experience in corporate and commercial matters, cross-border M&A, corporate finance, restructuring and private equity. He also regularly advises on fintech regulation, regulatory compliance, corporate governance, data protection, privacy and cybersecurity, and has acted for listed companies, multinational corporations, financial institutions, technology companies, private equity funds and start-ups.

Email: samwu@east-concord.com.hk



United States (California) - From Silicon Valley to Federal Scrutiny: Building AI, Data and Cybersecurity Governance Evidence

Sector Focus: AI Governance · Privacy · Cybersecurity · Board-Level Governance

U.S. technology governance does not operate through a single statute. For companies, the practical environment is a layered combination of state regulation, federal enforcement, securities disclosure, voluntary standards, consumer protection and private litigation. California shows this shift most clearly: governance is increasingly tested through records, risk assessments, audits, notices and escalation processes rather than policy statements alone.

California's 2025 privacy regulations, effective from 1 January 2026, introduced requirements covering risk assessments, cybersecurity audits and automated decisionmaking technology (ADMT). Covered businesses must be able to explain what personal information affects an automated decision, how outputs are used, whether meaningful human review exists and how consumer opt-out, access or appeal rights operate. Cybersecurity audit obligations are phased, with certification deadlines beginning on 1 April 2028 for businesses with annual gross revenue above US\$100 million. Senate Bill 53, signed on 29 September 2025, adds a frontier-AI layer by requiring large frontier developers to establish and publish frameworks addressing catastrophic-risk assessment, mitigation, incident response and internal reporting.

Federal governance reinforces the same evidentiary direction. NIST's AI Risk Management Framework remains voluntary but provides a common language for mapping, measuring and managing AI risk. The FTC's 2025 Workado order shows that claims about AI accuracy or effectiveness must be supported by competent and reliable evidence. For public companies, SEC cybersecurity rules require disclosure of material incidents on Form 8-K within four business days after materiality is determined, alongside annual disclosure of cybersecurity risk-management processes, board oversight and management responsibilities.

The recurring weakness is fragmentation inside the company itself. AI, privacy and cybersecurity are often managed as separate workstreams even when one product raises all three. Vendor assurances may be accepted without preserving supporting evidence, and "human-in-the-loop" controls may exist in name without giving reviewers real authority to change outcomes.

A more scalable approach is to maintain one governance baseline supported by an AI system inventory, use-case risk classifications, data maps, California risk-assessment files, cybersecurity audit records, ADMT notices and appeal processes, AI claims substantiation, vendor documentation, incident-materiality protocols and board reporting. The objective is not statutory uniformity across the United States, but evidence that can travel across regulators, customers, investors, acquirers and state-law overlays without rebuilding the governance system each time.

About the Author

SLLS Global Research Team

United States / United Kingdom - Whistleblowing, Data Protection, and Internal Controls as Evidence of Governance in Technology-Driven Companies

Sector Focus: Whistleblowing · AI Governance · Data Protection · Internal Controls · Board Oversight

Technology governance is tested not only by whether a company has policies, but by what happens when someone inside the organisation raises a serious concern. Reporting channels, escalation records, board papers and remediation logs can become the evidence by which regulators, courts, investors and counterparties judge whether governance actually worked.

Employees often see technology, data and compliance failures before boards or regulators do. Recent AI disputes reinforce that point. Concerns raised by current and former OpenAI and Google DeepMind employees in 2024 included calls for anonymous reporting channels to boards and regulators and protection against retaliation. California's Transparency in Frontier Artificial Intelligence Act, enacted on 29 September 2025 and effective from 1 January 2026, turns that governance principle into a documented process for large frontier developers: anonymous internal reporting of specified concerns, monthly status updates to the discloser, quarterly reporting to officers and directors, and penalties of up to US\$1 million per violation. The practical question becomes whether the company can produce the channel, the log, the escalation record and evidence of its response.

That approach is not unique to AI. Delaware oversight law has long tested whether boards established reporting systems and responded to what those systems revealed. *Marchand v. Barnhill* and *In re Boeing* illustrate why charters, minutes and management reports matter when directors later need to demonstrate oversight. Good intentions are difficult to defend if the governance record shows that material risks never reached the right forum or were repeatedly left unresolved.

The consequences of weak escalation can extend far beyond employment disputes. Howard Wilkinson made four internal reports concerning Danske Bank's Estonian operations in 2013 and 2014. Years later, Danske pleaded guilty and agreed to forfeit US\$2.059 billion, while the SEC reached a separate settlement of approximately US\$413 million. At Barclays, regulators fined chief executive James Staley an aggregate £642,430 after his handling of an anonymous whistleblowing letter and imposed special requirements on the bank, including annual reporting supported by personal attestation from its whistleblowers' champion. Wells Fargo provides an even sharper capital lesson: following widespread sales-practice failures and weaknesses in firm-wide risk management, the Federal Reserve restricted the bank's growth from 2018 until June 2025.

The common thread is not simply that wrongdoing occurred. It is that organisations already possessed information capable of exposing the risk, while their response-or lack of response-became part of the later regulatory record. This is why speak-up architecture increasingly matters in acquisition diligence, investment review and listing preparation. An acquirer or investor is unlikely to be satisfied by a whistleblowing policy alone; the more useful evidence is whether concerns were received, independently investigated, escalated, resolved and translated into changes in controls.

A workable governance system therefore needs relatively few but disciplined mechanisms. Speak-up should be a standing board or audit-committee item, with regular reporting on volumes, outcomes and closure times. Investigations should remain independent of the individuals implicated. Accountability can be strengthened through named attestations, while organisations should monitor what happens to reporters after concerns are raised. Most importantly, closing a case should include asking what the concern revealed about the underlying system and whether controls were changed.

For multinational technology companies, that evidence must also travel across borders. Local legal requirements, group-wide governance standards and the company's own commitments may not be identical, but the reporting architecture should remain credible wherever the concern originates. The decisive test is simple: when a material concern reaches the organisation, can the company later show who received it, who acted, what was decided and what changed?

About the Authors

James E. Miller

Partner, Miller Shah LLP · United States

James E. Miller represents institutional and individual clients in complex civil litigation, with particular experience in fiduciary disputes, securities and consumer class actions, and whistleblower matters. He also advises boards and management on investigations, internal reporting structures and governance issues arising from serious internal disclosures.

Email: jemiller@millershah.com



Georgina Halford-Hall

Chief Executive, WhistleblowersUK · United Kingdom

Georgina Halford-Hall works with parliamentarians, regulators, boards and investors on whistleblowing, governance and regulatory reform. Her work focuses on strengthening speak-up systems and treating whistleblowing as a mechanism for accountability and harm prevention rather than only as an employment dispute.

Email: ceo@wbuk.org



Part II – Europe

Opening Note - Proof Without Prescription



Sector Focus: Principles-Based Regulation · AI Governance · Open Finance · Board Accountability · Regulatory Proof

Switzerland offers a different answer to a question increasingly central to technology governance: how can trust be demonstrated when the law does not prescribe every operational step? Its model relies less on horizontal codification and more on technology-neutral statutes, supervisory expectations, institutional responsibility and evidence generated through governance itself.

Switzerland has deliberately avoided some of the comprehensive regulatory architecture associated with the European Union. There is no Swiss equivalent of the EU AI Act, nor a statutory requirement compelling banks to open interfaces to third-party providers. That should not be mistaken for a regulatory vacuum. The Swiss model places greater responsibility on firms, boards and control functions to translate broad legal duties into practical systems capable of being explained and defended.

The distinction is between prescription and proof. Prescriptive regulation defines requirements in advance and attaches standardised evidence to them: licences, conformity assessments, reporting templates and harmonised interfaces. Principles-based regulation defines objectives and duties of care while leaving more of the implementation to firms and supervisory practice. The trade-off is real. Prescription offers greater ex ante certainty and comparability but can be slower and more rigid; principles provide flexibility and speed but impose heavier self-responsibility and may produce less predictability. Neither approach is inherently superior.

Switzerland's constitutional framework helps explain that choice. Under Articles 5(1) and 164 of the Federal Constitution, state action requires a legal basis and significant rule-making must be grounded in formal legislation. Within that structure, Switzerland has generally preferred technology-neutral statutes supplemented by targeted sectoral reforms, such as the 2021 DLT amendments. FINMA then translates broader legal norms into supervisory expectations concerning governance, outsourcing, operational resilience and the fitness and propriety of institutions and their officers. The Federal Council has similarly chosen not to transpose the EU AI Act wholesale, favouring sector-specific instruments instead.

The consequence is that governance becomes the proof mechanism. A Swiss institution cannot rely solely on a certificate or checklist. It must be able to show how risks were identified, why decisions were taken, which controls were implemented, how deviations were detected and corrected, and who was accountable. Boards and senior management carry that burden directly. Demonstrability is therefore not an additional compliance layer attached after the fact; it is part of the institution's operating quality.

This model should not be described as "light-touch". Its credibility depends on whether market participants actually operationalise responsibility and preserve evidence of doing so. Where voluntary or principles-based systems fail to produce effective participation, accountability or control, pressure for more prescriptive regulation grows.

Open finance provides a useful test. Switzerland's market-driven model and the EU's PSD3/PSR framework pursue similar goals through different institutional machinery. The broader Swiss proposition is therefore conditional but clear: responsibility can substitute for prescription only where governance can be evidenced convincingly in practice.

Author: Peter Ruggle

Email: peter.ruggle@rugglepartner.ch

Switzerland - Open Finance as a Governance Laboratory: Switzerland's Market-Driven Path and PSD3/PSR



Sector Focus: Open Finance · Open Banking · Data Governance · Payments Regulation · Market Infrastructure

Open finance is not only a question of APIs and technical standards. It is a governance problem about who may access financial data, how customer authority is evidenced, how responsibility is allocated across the data chain, and what proof exists when access, security or transactions fail.

The European Union and Switzerland pursue broadly similar objectives but through different proof architectures. The EU relies primarily on prescription and harmonisation through PSD3 and the Payment Services Regulation (PSR), with the broader Financial Data Access Regulation still under negotiation. Switzerland has chosen a more market-driven model based on industry coordination, contractual arrangements, technical standards and regulatorily supervised self-responsibility.

The EU model formalises proof. Under the agreed PSD3/PSR architecture, entitlement to access follows regulatory status; customer consent is structured through prescribed authorisation processes and permission dashboards; security is supported by strong customer authentication, fraud-prevention duties and transaction monitoring; and liability is increasingly allocated directly through legislation, including refund rights and specified fraud scenarios. Interoperability is also treated as a regulatory deliverable rather than left to bilateral negotiation. The principal advantage is portability: licences, standardised controls and dashboards carry recognisable meaning across Member States. The corresponding cost is a slower legislative cycle and greater rigidity when business models change faster than regulation.

Switzerland has no statutory obligation requiring financial institutions to share customer data with third parties. That absence is deliberate rather than ungoverned. Since December 2022, the Federal Council has encouraged the industry to open interfaces without unjustified barriers while reserving the possibility of intervention if progress proves insufficient. A multibanking initiative involving approximately forty banks went live on 25 November 2025 through SIX's bLink platform, initially with limited participants and largely read-only functionality. In December 2025, the Federal Council acknowledged that progress remained uneven and moved toward measurable indicators against which further market development would be assessed.

Swiss proof therefore comes from a different combination of sources. The Federal Act on Data Protection governs processing and disclosure; banking secrecy under Article 47 of the Banking Act places strong weight on customer consent; platform participation and API relationships are governed contractually; FINMA expectations on outsourcing, resilience and ICT risk reach third parties through regulated institutions; and Common API specifications developed through industry coordination operate as a practical standard-setting layer.

The comparison is most consequential in liability and access. EU entitlement is clearer and more contestable because access follows legal status. Switzerland can move faster for participants already admitted to the ecosystem, but access remains dependent on market participation. EU law provides more direct statutory allocation of losses, while Switzerland relies more heavily on contract and general private law, which may work well between sophisticated institutions but leaves greater uncertainty in retail multi-party failures.

For firms operating across both systems, the practical response is not to build two unrelated compliance structures. A stronger baseline combines unified consent records, third-party governance, continuous audit trails, contractual liability allocation, board-level ownership and regulatory monitoring, with jurisdiction-specific proof layered on top.

Neither model is inherently superior. The EU tests whether formalisation can deliver portability without excessive rigidity; Switzerland tests whether market coordination can produce equally credible governance without statutory compulsion. The Swiss model remains viable only while participation, functionality, security and accountability can be demonstrated in practice.



About the Author

Peter Ruggle

Attorney at Law, Founding Partner, RUGGLE PARTNER · Switzerland

Peter Ruggle is a Swiss attorney whose practice includes corporate and commercial law, financial market regulation, corporate finance, transactions, litigation and arbitration. His work combines advisory and dispute-resolution experience with a longstanding focus on governance, financial services and the legal architecture supporting cross-border business.

Email: peter.ruggle@rugglepartner.ch



Germany - Observations on Contracting R&D on the Background of Global Knowledge Transfer



Sector Focus: R&D Contracting · International Knowledge Transfer · IP Management · Commercialisation · Innovation Strategy

International R&D cooperation can broaden access to knowledge, funding and markets, but collaboration alone does not produce innovation. Drawing on more than four decades of experience with R&D projects, including 35 years at Fraunhofer, the central lesson is that successful technology transfer depends on combining a clear research vision with disciplined IP management and a market-oriented international strategy.

Europe offers an exceptionally dense environment for research cooperation through EU and national funding programmes, including Horizon Europe. These programmes create extensive opportunities for universities, research institutions and companies to collaborate internationally, yet substantial research investment does not automatically translate into commercially successful products. In practice, the decisive step often occurs when an institution or company takes responsibility for converting research results into something the market can actually use.

Different regions illustrate different strengths. North America benefits from close university–industry links and strong industrial research capacity. Asia-Pacific markets, in the author's experience, have often demonstrated particular speed in translating technological knowledge into marketable products. China combines strategic state direction, research capacity and industrial execution, while wider Pacific frameworks support mobility, intellectual property activity and industrial cooperation. The broader point is not that one regional model is superior, but that international knowledge transfer creates value only when the receiving organisation has the capacity and incentives to commercialise it.

For R&D contracting, professional IP management is therefore fundamental from the beginning. Parties should identify relevant background knowledge, secure sufficient IP-management resources, define the research objective and consider the likely commercial market. International collaborations also require attention to ownership rules attached to public funding, confidentiality between potentially competing partners, exploitation rights, patentability and infringement risk. Licensing adds further complexity because procedures, fees, territorial controls and import or export restrictions may vary significantly across jurisdictions.

Three examples from Fraunhofer illustrate how these factors operate differently. The development of MP3 began in 1983 with a small research team and ultimately succeeded through sustained technical work, institutional support, international standardisation and commercialisation with industry. The path, how the flat screen technology found its way to the market points to a different lesson: technological readiness and an adequate IP position may still fail to produce domestic commercial success where the investment appetite required for market entry is absent. By contrast, Asian manufacturers demonstrated the capacity to move quickly from available technological knowledge to large-scale production. Actually, strong efforts of Research Work bringing dandelion-based rubber on the market shows a third pattern, where know-how and trade secrets may matter more than patents, while market entry can still be delayed by production economics or other commercial barriers.

These cases suggest that no universal innovation model exists. Public funding, international cooperation, research excellence and IP protection can all contribute, but the route from laboratory to market remains highly dependent on timing, investment, competitive dynamics and commercial demand.

For companies and research institutions, three disciplines stand out: a concrete researcher vision, professional IPR management, and a market-driven international strategy. International cooperation is most valuable when these elements are already embedded in the project rather than added after the research is complete. The practical purpose of an R&D contract is therefore not merely to organise collaboration, but to preserve the rights, incentives and commercial pathways needed for knowledge to become an innovation that survives in the market.



About the Author

Dr. Lorenz Kaiser

Lawyer (R&D Contracting and IPR)
Senior Legal Counsel, GE Aviation
Germany

Dr. Lorenz Kaiser has more than four decades of experience in R&D contracting, technology transfer, intellectual property management and innovation commercialization. He spent approximately 35 years with the Fraunhofer-Gesellschaft, working across research cooperation, IP strategy and the transfer of applied research into industry. His work reflects long-standing engagement with international R&D projects, licensing, standardization and the conditions required to move technological knowledge from research into marketable products.

Email: mail@lorenz-kaiser.de, lorenz.kaiser@geaerospace.com



Germany - The Use of AI in Management and Supervisory Bodies: Finding the Right AI Governance Framework for Corporate Leadership

Sector Focus: Board-Level AI Governance · Directors' Duties · Supervisory Boards · Corporate Liability · Human Oversight

AI is moving into management and supervisory decision-making, but German company law does not impose a general duty on directors to use it. The more important question is how AI changes the existing standard of care and whether its use, or misuse, creates new liability for management and supervisory bodies.

German corporate law remains technology-neutral. Whether operating through an AG, GmbH or other legal form, management must comply with established duties including legality, loyalty and the diligence of a prudent and conscientious manager. Section 93(1) AktG sets that standard for management board members of stock corporations, while section 43 GmbHG applies correspondingly to GmbH directors and section 116 AktG extends the standard to supervisory board members. AI may support decision-making, document validation or risk assessment, but directors retain discretion over whether and how it is used.

That discretion requires discipline. Before deploying AI, directors should consider whether the tool is suitable for the task, how company or third-party data will be handled, whether trade secrets are exposed, and whether the organisation has an agreed governance process. Once AI is used, outputs should be checked for plausibility and hallucination, and the human decision-making step should remain identifiable.

AI also interacts with Germany's principle of collective management responsibility. A valid allocation of portfolios within the management boards does not eliminate each director's residual monitoring duties with regard to the portfolios of other directors. The Federal Court of Justice confirmed this in its decisions of 6 November



2018 (II ZR 11/17) and 14 March 2023 (II ZR 162/21): directors remain responsible for monitoring developments outside their assigned areas where circumstances require intervention. AI can make information from colleagues' portfolios easier to access and test, creating a new governance question-when should that additional visibility trigger escalation, and how should such review be controlled?

The same issue is particularly significant under Germany's dual-board structure. Supervisory boards have a statutory duty under section 111(1) AktG to supervise management. Under the ARAG/Garmenbeck line of authority, once a well-founded claim against management is identified, the supervisory board generally has little discretion simply to ignore it. Rather, claims for compensation for damages must, as a matter of principle, be brought against directors where they are liable. This applies with particular rigour in the case of German public limited companies. AI-assisted oversight may therefore increase the amount of information available to supervisory boards, while simultaneously increasing the need to validate findings, share them appropriately and document decisions on escalation or enforcement.

A workable response is a written AI governance framework tailored to corporate organs. It should identify approved tools and permitted use cases, establish rules for sensitive data, require validation of AI-supported findings, preserve the human decision step, and define escalation between directors, supervisory board members and specialist functions. Portfolio allocations should remain clear and genuine, and AI-assisted monitoring of other areas should follow protocol rather than ad hoc initiative.

German law does not require boards to become AI-driven. It does require them to remain capable of exercising informed, independent and documented judgment as AI becomes part of corporate decision-making. The governance challenge is therefore to use AI where it improves oversight without allowing the technology itself to obscure responsibility.

About the Author

Andreas Hecker, LL.M. oec.

Rechtsanwalt · Partner, Hoffmann Liebs · Düsseldorf, Germany

Andreas Hecker advises listed and non-listed companies on corporate governance, directors' and officers' responsibilities, capital markets law, corporate reorganisations, compliance and M&A. He also represents clients in related corporate litigation and has long-standing experience advising on internal organisation and reporting structures. He has been a Partner at Hoffmann Liebs since 2016 and regularly lectures and publishes on corporate and corporate group law.

Email: andreas.hecker@hoffmannliebs.de



Hungary - Proof Before Prompt: Closing the AI Governance Gap in Hungarian SMEs



Sector Focus: AI Governance · SME Compliance · Data Protection · Trade Secrets · AI Literacy

Hungarian SMEs are adopting AI faster than their internal governance systems are developing. The immediate risk is not simply whether new AI rules apply, but whether companies can identify where AI is already being used, what information employees are entering into those tools, and who is responsible for controlling that use.

Enterprise-level AI adoption in Hungary remains below the EU average. Eurostat data for 2025 recorded AI use by 20.0% of EU enterprises with ten or more employees, compared with 10.37% in Hungary; among Hungarian small enterprises the figure was 8.7%, rising to 15.3% for medium-sized companies. Those figures do not capture widespread informal use by employees who draft contracts, translate correspondence or prepare quotations using generative AI, often through personal accounts and without an approved policy or designated owner.

The regulatory timetable has also created false comfort. The EU AI Act has applied in stages since 2 February 2025, when prohibited practices and AI literacy obligations began to apply. General-purpose AI model obligations followed on 2 August 2025, while later implementation dates were recalibrated by the 2026 Digital Omnibus. For SMEs, however, postponement of certain high-risk-system obligations does not remove the risks already arising from everyday AI use. Article 4 AI literacy obligations and Article 50 transparency requirements remain relevant, while GDPR duties, confidentiality obligations and trade secret protection continue independently.

The most common governance gap is “shadow AI”: employees adopting tools without approval, inventories or management visibility. This can create four recurring exposures. Confidential information entered into public AI tools may breach NDAs at the point of disclosure. Internal methodologies, algorithms or templates entered

without control may undermine the “reasonable steps” required to preserve trade secret protection under Hungarian and EU law. Personal data entered into AI tools remains fully subject to the GDPR: lawful basis, transparency, controller/processor roles, security and retention apply from the moment of input. Reliance on hallucinated outputs can also create contractual, employment and reputational consequences where human review is absent.

These risks increasingly matter beyond compliance. AI use, data handling and trade secret protection now appear in M&A and financing diligence, where undocumented practices can affect pricing, warranties and closing. Larger customers and international partners may also impose governance expectations contractually before statutory deadlines require them.

For Hungarian SMEs, the proportionate answer is not a large-enterprise compliance structure. A trained internal AI Officer can provide a practical control point: maintaining the tool and use-case inventory, assessing new systems and vendors, updating policy and audit trails, and acting as the internal contact for employee questions. Supporting measures can remain simple—a short AI policy, a prohibited-input list covering personal data, client information, pricing, source code and know-how, an approved-tools list, supplier due diligence, basic AI literacy training, and a simple inventory of tools, processes and data categories.

The central principle is visibility before control. A company cannot govern AI use it does not know exists. For Hungarian SMEs, demonstrable governance now depends less on complex documentation than on assigning ownership, training employees and maintaining an audit trail that can be shown to regulators, investors and business partners when asked.

About the Author

Dr. Zita Kósa-Lantos

Data Protection & AI Governance Expert, ESG Consultant, ESG-GDPR e.U. · Hungary / Austria

Dr. Zita Kósa-Lantos is a Hungarian legal expert and certified ESG Specialist Lawyer with more than 20 years of experience in data protection, GDPR compliance and privacy governance. She formerly headed the Data Protection Department at Hungary's National Health Insurance Fund and now advises SMEs and municipal companies on data protection, AI governance, audits, internal training and EU AI Act readiness. She is the Founder of ESG-GDPR e.U. in Austria and Head of AI Legal at InstaPrice.ai.

Email: office@esg-gdpr.eu



Poland - Proof Before Scale: Building an EU-Ready Compliance Architecture for China-Headquartered Technology Companies



Sector Focus: EU Market Entry · Cyber Resilience · Data Governance · AI Compliance · Proof Architecture

For China-headquartered technology companies entering the European Union, regulatory readiness increasingly depends on whether legal responsibility, technical reality and supporting evidence can be connected before launch. Compliance must be capable of being produced quickly, not reconstructed after scrutiny begins.

European technology regulation is increasingly creating operational evidence requirements. The Cyber Resilience Act illustrates the shift: since 11 September 2026, its Article 14 reporting regime has required rapid escalation of actively exploited vulnerabilities and severe incidents, with an initial warning potentially due within 24 hours and a further notification within 72 hours. The Data Act creates a parallel product-design challenge by requiring relevant product and related-service data to be accessible to users. The AI Act and GDPR reinforce the same direction through documentation, accountability, oversight and international-transfer requirements.

For China-to-EU expansion, the central difficulty is often organisational rather than legal. R&D, source code, technical documentation and cybersecurity teams may remain in China while the EU subsidiary, importer or distributor carries local obligations. Cloud infrastructure and remote access can add further complexity. The risk arises when the entity with the legal duty does not control the information needed to discharge it.

A workable proof architecture connects those two sides before scale. It begins with an accurate product and data-flow map showing software components, cloud dependencies, AI-enabled features, data generation, remote access and third parties. Legal roles should then be mapped to named entities and responsible people so that manufacturers, importers, distributors, controllers, processors and other actors can obtain the informa-

tion they need when deadlines begin to run.

Incident readiness should be designed around the first 24 hours. Engineers do not need to become regulatory lawyers, but they need clear escalation triggers so that vulnerability reports, monitoring alerts or customer complaints reach the correct security and legal contacts immediately. Contracts must also carry information, not merely allocate liability: EU entities should have enforceable rights to obtain technical documentation, vulnerability information, update records and cooperation from headquarters, developers and service providers.

The final layer is a controlled evidence file containing current product architecture, regulatory-role matrices, technical documentation, cybersecurity assessments, software-dependency records, data-transfer materials, key contracts, test results and significant compliance decisions, with effective version control.

The commercial value extends beyond enforcement. Customers, investors, acquirers, insurers and strategic partners increasingly test the same evidence during procurement and diligence. For China-headquartered technology groups, the practical lesson is therefore straightforward: EU compliance should be built into the operating model before launch. Proof should precede scale, not be reconstructed after it.

About the Authors

Paweł Sikora

Partner, KKG Legal · Head of New Technologies & Start-ups (TMT)

Paweł Sikora advises on corporate, transactional, employment and cross-border matters and coordinates KKG Legal's China-related activities through its Shenzhen Representative Office. He regularly supports Chinese companies entering and developing their business in Poland and helps bridge legal, regulatory and commercial requirements between China and Europe.

Email: pawel.sikora@kkg.pl



Dominik Gałkowski

Co-managing Partner, KKG Legal · Leader of the Environmental Protection and Sustainable Development Practice

Dominik Gałkowski has participated in advisory teams supporting legislative reform and serves as an arbitrator with the Guangzhou Arbitration Commission and Hainan International Arbitration Court. His professional work combines regulatory, institutional and cross-border dispute perspectives.

Email: dominik.galkowski@kkg.pl



Part III – Southeast Asia

Opening Note - Governing Scale Across Fast-Moving Digital Markets

Southeast Asia is entering a more demanding phase of digital growth. Technology adoption remains rapid, but the governance question is changing. Companies are no longer judged only by whether they can launch, connect and expand. They are increasingly expected to show how data are handled, how AI is supervised, how intellectual property is protected, how technology suppliers are controlled and how responsibility is allocated when systems fail.

The region matters because regulatory development is occurring alongside commercial scale. Indonesia is strengthening the connection between AI governance, data protection and transaction readiness. Malaysia is addressing technology risk through both contract design and emerging debate over copyright, AI training and text-and-data mining. Cambodia shows a different stage of development, where trade-secret protection, contractual safeguards and internal controls remain particularly important as the digital economy expands.

These differences make a single regional compliance model unrealistic. The more useful approach is to build a common governance core-clear ownership, data mapping, vendor controls, cybersecurity obligations, AI-use oversight, IP protection and documented escalation-while adapting the legal layer to each jurisdiction.

For cross-border businesses, the practical challenge is therefore interoperability without losing accountability. A technology contract should be capable of travelling across markets without obscuring local obligations. AI systems should be scalable without losing visibility over data, outputs and human responsibility. Intangible assets should remain identifiable and defensible as development, hosting and commercialisation cross borders.

Southeast Asia's next phase of digital growth will depend less on the speed of adoption alone and more on whether companies can demonstrate that growth remains governable. The strongest businesses will be those able to convert legal requirements, contractual expectations and technical controls into evidence that investors, regulators, customers and counterparties can understand and trust.



Indonesia - Towards Responsible AI: A Governance Framework for the Digital Age

Sector Focus: AI Governance · Data Protection · Investor Due Diligence · Digital Economy · Corporate Transactions

Indonesia's AI-specific regulatory framework is still developing, but companies cannot treat that uncertainty as a governance safe harbour. For investors and acquirers, the immediate question is increasingly whether an AI-enabled business can produce evidence showing who owns AI risk, what data its systems use, and how incidents and regulatory exposure are managed.

The binding baseline is already in place. Indonesia's Personal Data Protection Law, Law No. 27 of 2022, has been fully effective since 17 October 2024 and has extraterritorial reach in specified circumstances, although establishment of the dedicated supervisory authority remains ongoing. Meanwhile, a National AI Roadmap and a separate AI Ethics and Safety Presidential Regulation have cleared inter-ministerial review and await presidential approval. Sector-specific rules are expected to follow, with the Ministry of Communication and Digital Affairs having prepared an AI-generated-content labelling regulation for release after the Presidential Regulation is signed.

This distinction matters in transactions. A Presidential Regulation cannot itself impose criminal or administrative sanctions under Indonesian law, so the proposed AI framework is expected to operate principally as



a standards-setting instrument. Existing laws, particularly the PDP Law and the Electronic Information and Transactions Law, remain the immediate sources of legal exposure. Regulatory uncertainty therefore affects diligence rather than suspending it.

Investors are already examining AI and data governance in Indonesian technology transactions. Governance gaps can lead to more intensive diligence, longer transaction timetables and pressure on valuation, and may ultimately appear in transaction terms through escrow arrangements or indemnities. Buyers and sellers also need to distinguish clearly between obligations already binding and requirements that remain prospective when negotiating compliance representations and warranties.

A practical response is the Govern – Prove – Scale framework. Govern begins with named accountability: each AI system should have an identifiable individual owner, use cases should be classified according to risk, and higher-risk systems should include a person with real authority to pause, review or override outcomes. Prove means creating the evidence contemporaneously. For AI systems processing personal data, this includes documenting the lawful basis and conducting a DPIA-style assessment, while maintaining incident and breach records and incorporating governance obligations and audit rights into third-party AI contracts.

Scale turns those controls into a diligence-ready governance file. At minimum, this should contain a board-approved AI governance policy, an AI systems register with risk classifications, relevant DPIAs or equivalent impact assessments, incident and remediation records, AI-vendor governance provisions, and evidence of periodic board or committee oversight. Alignment with the ASEAN Guide on AI Governance and Ethics can provide an additional regional reference point for investment committees less familiar with Indonesia's evolving framework.

The advantage lies less in elaborate process than in consistency, traceability and retrievability. A company that can produce its governance record when diligence begins is in a materially different position from one promising to create it after the regulatory framework settles. In Indonesia's developing AI market, governance evidence increasingly supports not only compliance, but transaction readiness and investor confidence.

About the Author

Jade Hwang

Foreign Consultant, Nusantara DFDL Partnership · Indonesia

Jade Hwang advises on cross-border M&A, joint ventures, corporate restructuring, capital markets and securities matters. Her regional practice experience spans Indonesia, Malaysia and Cambodia, and she advises clients across sectors including technology, healthcare, retail, real estate, energy and resources, financial institutions and venture capital. She is currently based in Indonesia.

Email: Jade.Hwang@dfd.com



Malaysia - Technology Contracts That Scale: Managing Data, Intellectual Property and AI Risks in Cross-Border Collaborations

Sector Focus: Cross-Border Technology Contracts · Data · IP · AI · Cybersecurity

Technology contracts increasingly determine whether cross-border technology relationships can grow without creating uncertainty over ownership, data use, AI deployment, cybersecurity and regulatory responsibility. For Malaysian businesses, the central drafting challenge is to allocate these risks before technology, information and services begin moving across jurisdictions.

Technology agreements now do more than record price, scope and delivery. A Malaysian company may use an overseas cloud provider, deploy a foreign AI platform, outsource software development and process personal data across several jurisdictions at the same time. Each activity may create different legal and contractual consequences, so the agreement must be designed for both the present transaction and the business model the parties expect to operate as the relationship expands.

Intellectual property should be addressed with precision. The contract should distinguish background IP, foreground IP, third-party IP, and improvements or derivative works rather than assume that payment for development resolves ownership. Where foreground IP is created, the agreement should state whether it is assigned, jointly owned or licensed and define permitted use, territory, duration, exclusivity, sublicensing and commercialisation rights. Cross-border projects may also require additional assignments, registrations or other formalities in relevant jurisdictions.

Data requires a different analysis. The practical question is often not simply who “owns” data, but who may access, process, transfer, analyse or reuse it. Malaysia’s Personal Data Protection Act 2010, as amended by the Personal Data Protection (Amendment) Act 2024, came into operation in stages on 1 January, 1 April and 1 June 2025. The Personal Data Protection Commissioner’s Guidelines on Cross-Border Transfer of Personal Data address transfers outside Malaysia under section 129 of the PDPA. Contracts involving cloud, SaaS or AI services should therefore deal expressly with data categories, processing purposes, storage locations, onward transfers, subcontracting, security, retention, deletion, breach cooperation and audit rights. They should also clarify whether customer data may be aggregated, anonymised, analysed, used to improve services or used to train a provider’s AI model.

Generative AI adds contractual uncertainty that conventional ownership and confidentiality clauses may not fully resolve. Malaysia currently has no single statute governing generative AI across all sectors. The National Guidelines on AI Governance and Ethics and the Voluntary AI Code of Ethics remain non-binding, but their principles can be translated into contractual obligations. Parties



should consider whether AI may be used at all, which models or platforms are permitted, whether confidential or customer information may be submitted to third-party systems, whether data may be retained or used for model improvement, who may exploit AI-generated outputs, whether human review is required, and how responsibility is allocated for inaccurate or infringing material. A simple clause stating that “all deliverables belong to the customer” may be insufficient where deliverables incorporate open-source software, third-party components or AI-generated material subject to separate licence restrictions.

Cybersecurity should be treated with equal specificity. General language requiring “appropriate security measures” may offer little guidance when an incident occurs. Agreements may instead define obligations covering encryption, access management, multi-factor authentication, vulnerability management, penetration testing, incident response, business continuity, disaster recovery, subcontractor controls and security audits. Malaysia’s Cyber Security Act 2024 reinforces cybersecurity as a formal regulatory and contractual concern, although not every technology agreement falls within the National Critical Information Infrastructure framework.

Cross-border transactions also require more than a Malaysian governing-law clause. Foreign laws may remain relevant because of customer location, servers, data processing, subcontractors, IP creation or exploitation, or regulatory investigations. Responsibility for licences, approvals, consents, data-protection compliance, regulatory enquiries and subcontractor obligations should therefore be allocated expressly.

For scale, a master technology agreement supported by modular schedules for IP, data protection, cybersecurity, AI governance, service levels, technical specifications, change management and business continuity can preserve a consistent risk allocation while allowing the relationship to evolve. Exit provisions should also address data return or deletion, migration assistance, source-code or documentation access where agreed, termination of licences and continuing confidentiality. The practical test remains whether the contract clearly answers five questions: who owns the technology, who may use the data, how AI may be used, who is responsible when security fails, and who bears the legal and financial consequences when something goes wrong.

About the Author

Yong Siew Lee

Managing Partner, YONG SL & KOH, Advocates & Solicitors · Malaysia

Ms. Yong Siew Lee is the Founder and Managing Partner of Messrs Yong SL & Koh. She has been practising law since 2012 and specialises in corporate and commercial law, cross-border investments, joint ventures and mergers and acquisitions, transaction structuring, technology and cybersecurity, corporate compliance, and commercial dispute resolution. She is an international commercial lawyer and qualified mediator, and has been appointed as a lecturer by the Guangdong-Hong Kong-Macao Greater Bay Area Foreign Involvement Lawyer Academy. She also serves as legal consultant to various other professional and business organisations.

Email: siewlee@yklaw.com.my



Malaysia - Considers Reforming Copyright Laws to Deal with AI Challenges



Sector Focus: AI & Copyright · Text and Data Mining · Licensing · Data Protection · Cultural Heritage

Malaysia is considering how copyright law should respond to the use of protected works in AI training without undermining creators' rights or the country's wider AI ambitions. The policy question is not simply whether to permit text and data mining, but how any exception should interact with licensing, personal data protection and cultural heritage safeguards.

Malaysia currently has no AI-specific copyright provision. The legality of AI training therefore falls within the existing Copyright Act 1987, under which copyright owners retain exclusive rights including reproduction, communication, distribution and commercial exploitation. Existing exceptions, including fair dealing under section 13(2)(a) and transient electronic copying under section 13(2)(q), provide limited certainty for AI training. While temporary copies created in computer memory may fall within the transient-copying exception, AI training commonly involves pre-processed datasets and cached files retained for fine-tuning or retraining, taking the process beyond purely temporary reproduction.

The issue moved closer to formal reform when the Intellectual Property Corporation of Malaysia (MyIPO) released a public consultation in July 2026 on proposed amendments to the Copyright Act 1987. One possible reform is a text and data mining (TDM) exception for AI training. The consultation identifies concerns around unauthorised use of copyrighted works, licensing and consent mechanisms, transparency of training datasets, and unauthorised use of a person's voice, image or performance.

Comparative approaches point in different directions. Japan adopts a purpose-based model that permits AI training for information analysis where the use does not unreasonably prejudice copyright owners. Singapore uses a lawful-access model, allowing TDM for computational analysis where the material has been lawfully accessed and restricting rights holders from excluding such use contractually. These models offer useful reference points, but Malaysia's domestic legal framework makes a broad exception more complex.

AI training datasets may contain personal information governed by the Personal Data Protection Act 2010, including material collected from websites, user-generated content or biometric data. Malaysia's cultural heritage regime also matters. The National Heritage Act 2005 covers traditional cultural expressions such as songs, music, dances and performing arts, while section 51(3) recognises that copyright-owner consent remains necessary where copyright subsists in relevant heritage material. Any TDM exception would therefore need to operate alongside existing copyright, data protection and cultural heritage safeguards.

Policy statements in 2026 also indicate a preference for balance rather than unrestricted access. Digital Minister Gobind Singh Deo emphasised data sovereignty and the needs of local industries, while Deputy Minister Datuk Fuziah Salleh stated that copyrighted works used for AI training require approval, licensing and royalty arrangements, with creators' interests given priority.

A calibrated model would therefore appear more consistent with Malaysia's current policy direction than the broadest possible TDM exception. Such an approach could permit the use of lawfully accessed works for legiti-

mate AI development while incorporating safeguards on transparency, consent, licensing, opt-out mechanisms, personal data and cultural heritage. Additional controls may also be appropriate where training makes substantial use of copyrighted works or could affect the market for the original material.

Licensing should remain central rather than be displaced by reform. It can provide AI developers with access to quality datasets while allowing copyright owners to retain control and receive compensation. A limited TDM exception combined with licensing and targeted safeguards would give both developers and rights holders greater certainty while supporting AI development without weakening the domestic creative and cultural ecosystem.

About the Authors

Stanley Lee Wai Jin

Partner, Zaid Ibrahim & Co · Malaysia

Stanley heads the Intellectual Property practice group at Zaid Ibrahim & Co. He has more than a decade of experience in corporate and commercial matters including intellectual property, franchise registration, personal data protection, telecommunications, media and technology, and has advised clients across multiple industries and jurisdictions. He also has litigation and anti-counterfeiting enforcement experience.

Email: stanleylee@ziclegal.com



Ashley Ng Kai Yee

Associate, Zaid Ibrahim & Co · Malaysia

Ashley is an Associate in the Intellectual Property practice group at Zaid Ibrahim & Co. Her work focuses on the prosecution of trademarks, patents, copyright and industrial designs, together with intellectual property litigation, dispute resolution and pre-trial negotiations.

Email: ashleyng@ziclegal.com



Cambodia - Trade Secrets as Technology Governance: Safeguarding Innovation and Investor Confidence in Cambodia's Digital Economy



Sector Focus: Trade Secrets · Technology Governance · Investor Due Diligence · Digital Economy · IP Protection

As Cambodia expands its digital economy, confidential technological and commercial information is becoming a larger part of enterprise value. The challenge is that businesses increasingly depend on trade secrets while Cambodia still lacks a standalone statutory framework dedicated to their protection.

Cambodia's policy direction strongly supports digital transformation, innovation and private-sector development through the Cambodia Digital Economy and Society Policy Framework 2021–2035, the STI Roadmap 2030 and the Pentagonal Strategy – Phase 1 (2023–2028). As fintech, e-commerce, business process outsourcing, logistics technology, agritech, artificial intelligence and software development expand, competitive advantage increasingly depends on intangible assets such as source code, proprietary algorithms, customer databases, pricing models, AI training data, manufacturing know-how, cybersecurity procedures and business strategies.

The legal framework for protecting those assets remains fragmented. Cambodia has established laws covering trademarks, copyright, patents, industrial designs and geographical indications, but no dedicated trade secrets statute. Businesses therefore rely heavily on contractual measures such as non-disclosure agreements and employment confidentiality clauses. Limited statutory protection may indirectly arise through Article 22 of the Law on Marks, Tradenames and Acts of Unfair Competition, while Article 39 of the TRIPS Agreement protects undisclosed information where it remains secret, derives commercial value from its secrecy and has been subject to reasonable protective measures.

A significant policy development came on 18 February 2025, when the Department of Intellectual Property Rights under the Ministry of Commerce presented a draft Law on Trade Secrets at a national seminar. The draft is anticipated for formal enactment by 2027. The proposed legislation is important because uncertainty over protection and enforcement can affect not only dispute outcomes but investment decisions, particularly where

businesses depend on proprietary data, research results or confidential technology.

Current enforcement routes remain imperfect. Trade secret disputes may be addressed through Preliminary Alternative Dispute Resolution before the DIPR, national courts or the National Commercial Arbitration Centre. PADR may offer a faster and less costly route to settlement, but the DIPR's procedural role and authority are not expressly regulated for trade secret disputes. Court proceedings may be lengthy and costly and lack specialist IP treatment, while enforcement of an arbitral award through the NCAC may still require assistance from the Court of Appeal.

This legal uncertainty can also affect collaboration between public institutions, universities and private investors. The Institute of Technology of Cambodia, for example, generates technological innovation through students and researchers supported by government funding, yet private capital may remain cautious where ownership transfer, confidentiality and remedies for misuse are unclear. More predictable protection could therefore support collaborative R&D as well as investor confidence.

For technology companies, trade secret protection should be treated as a governance function rather than only an IP issue. The commercial value of confidential information depends on whether the organisation can demonstrate how it is identified, accessed, stored, shared and protected. Investors increasingly examine these controls during due diligence alongside formal ownership of intellectual property.

Practical preparation should begin before a dispute or investment process. Companies should identify and classify confidential information by commercial value and sensitivity; adopt policies covering ownership, authorised access, storage, use, disclosure and disposal; and combine dual-language NDAs with technical access controls, cybersecurity measures and disciplined offboarding procedures. Documented incident-response mechanisms and periodic trade-secret audits should test access permissions, contractual protections, employee compliance, third-party disclosures and technical safeguards.

Until Cambodia's dedicated statutory framework matures, the strongest protection will depend on both legal rights and demonstrable internal controls. Companies that can show disciplined governance over confidential assets will be better positioned to protect enterprise value, support R&D collaboration and give investors greater confidence in the resilience of their technology operations.

About the Author

Songmeng Chhorn

Managing Partner, MENG & ASSOCIATES · Cambodia

Songmeng Chhorn is the Managing Partner of MENG & ASSOCIATES, a Phnom Penh-based law firm he has led for nearly a decade. He advises SMEs and foreign investors on corporate law, investment structuring and cross-border transactions, with a practice focused on practical legal solutions in Cambodia's evolving business environment.

Email: meng@meng.legal



Part IV – South Asia

Opening Note - At the Frontier of Digital Public Infrastructure: Operationalizing “Proof First, Scale Fast”



South Asia has emerged as one of the world's most dynamic testbeds for digital transformation. Driven by the aggressive deployment of Digital Public Infrastructure (DPI), unified real-time payment interfaces, and rapid consumer adoption of data-driven and AI services, the region is leapfrogging traditional development paradigms. Emerging market corridors such as the expanding Nepal-India cross-border digital financial linkage demonstrate how regional integration is no longer merely physical, but deeply algorithmic and data-dependent.

However, this rapid digital acceleration exposes a fundamental structural vulnerability across South Asian jurisdictions. Historically, market expansion in technology followed a “scale first, correct later” doctrine. In the domains of financial technology, cross-border data flows, and artificial intelligence, this legacy playbook is no longer viable. Operating across heterogeneous regulatory environments where legislative frameworks are either rapidly shifting or still pre-statutory presents immediate legal exposures: regulatory friction, cross-border asset freezes, capital control evasions, and jurisdictional conflict.

Across fintech, AI, and data governance, South Asia faces three interconnected governance challenges:

- **Monetary Sovereignty vs. Cross-Border Integration:** The imperative to connect retail payment switches across borders frequently collides with national central bank directives on data localization, currency stability, and capital flow restrictions.
- **Regulatory Asymmetry & Pre-Statutory Exposure:** Commercial adoption of artificial intelligence and automated decision-making is outpacing statutory legislation. Operating in regulatory silences exposes market actors to severe contractual, penal, and reputational risk before formal acts are promulgated.



- Shift from Permission-Seeking to Responsive Compliance: Modern data protection frameworks across the region are shifting away from rigid prior-authorization regimes toward dynamic, risk-based compliance demanding continuous organizational adaptation rather than static legal approvals.

To bridge the gap between rapid technological expansion and legal certainty, this section posits a unifying doctrine: “Proof First, Scale Fast.”

Under this framework, market actors and regulators must establish architectural, algorithmic, and contractual “proof of governance” prior to commercial scaling. Rather than viewing compliance as a post-hoc legal audit, “Proof First, Scale Fast” embeds regulatory requirements directly into technical and legal infrastructure. This includes adopting split-node data architectures that preserve domestic residency while enabling cross-border clearing, deploying programmatic capital controls directly into payment switch payloads, utilizing standardized Data Processing Agreements (DPAs) in pre-statutory environments, and integrating institutional arbitration into cross-border technology contracts for neutral, expert dispute resolution.

The contributions in this edition evaluate these exact frontiers across the South Asian landscape. By shifting from retroactive compliance to privacy-and-governance-by-design, South Asia can establish an auditable, resilient foundation for cross-border digital trade scaling market access rapidly without sacrificing sovereign trust or legal integrity.

About the Author

Upendra Raj Dulal

Advocate & Partner | Authorized Translator, Agrani Law Associates; Faculty Member, Nepal Law Campus, Tribhuvan University · Nepal

Upendra Raj Dulal is a Partner at Agrani Law Associates specializing in International Trade, Foreign Direct Investment (FDI), and Arbitration. Holding an LLM in International Law from Wuhan University, he acts as a strategic counsel for global investors, with deep regional expertise across Asian markets. Upendra advises international enterprises on cross-border contract negotiations, investment law, and complex regulatory compliance, providing end-to-end due diligence and arbitration representation to safeguard foreign investments in Nepal. Additionally, he serves on the faculty at Nepal Law Campus, Tribhuvan University.

Email: dulalupendra@yahoo.com



India - Cross-Border Data Governance in India: Making Digital Trust Scalable under the Digital Personal Data Protection Framework



Sector Focus: Cross-Border Data · Data Protection · Digital Trust · Board Governance · Regulatory Readiness

India is moving toward a cross-border data model in which openness is the default and government restriction is the exception. For companies, that shifts the governance question from obtaining permission for each transfer to proving that data flows, contractual safeguards and contingency arrangements can be identified and adapted if the regulatory position changes.

Section 16 of the Digital Personal Data Protection Act 2023 establishes a negative-list structure: once the provision comes into force, personal data may be transferred outside India unless the Central Government restricts such transfer to a specified country or territory. The Digital Personal Data Protection Rules, 2025, notified by the Ministry of Electronics and Information Technology in November 2025, provide the accompanying regulatory framework. The Act and Rules are subject to a phased commencement, with Sections 11 to 17 of the Act, including Section 16, scheduled to come into on 13 May 2027. Accordingly, the cross-border transfer regime described here should be understood as the statutory framework established by the Act and Rules and as subject to their notified commencement timeline. As of the date of this article, no restricted destination had been designated under Section 16.

That general openness does not eliminate future localisation risk. Once the relevant provisions come into force, Rule 13(4) will require a Significant Data Fiduciary to ensure that personal data specified by the Central Government, on the basis of recommendations of a committee constituted for that purpose, together with traffic data pertaining to the flow of such data, is not transferred outside the territory of India. Sectoral requirements also continue independently. Reserve Bank of India rules on payment-system data, together with requirements applying in securities and insurance, may impose obligations that are separate from the horizontal DPDP framework. A company can therefore satisfy the general transfer regime while remaining subject to a sector-specific residency rule.

India's model also differs materially from neighbouring approaches. Mainland China requires outbound personal information to move through defined mechanisms such as security assessment, standard contracts or certification, depending on applicable conditions and thresholds. Hong Kong's section 33 cross-border transfer provision under the Personal Data (Privacy) Ordinance has never been brought into force, although the Privacy Commissioner has issued guidance encouraging organisations to prepare for the eventual operation of the provision. For businesses operating across India, mainland China and Hong Kong, identical data flows may therefore require different governance evidence rather than a single regional transfer policy.

This matters directly to investment and commercial diligence. A target dependent on overseas cloud infrastructure may face contingent exposure if a destination is later restricted. Investors and acquirers increasingly need visibility into where data travels, which vendors receive it and whether systems can be migrated without disrupting operations. Responsibility also continues after transfer: the Data Fiduciary's accountability does not end merely because personal data has crossed India's borders.

A practical governance model begins with a living data-flow inventory covering categories of personal data, vendors, cloud regions and business purposes. Contracts should contain migration rights, data-portability obligations, exit assistance and sector-specific safeguards rather than assume that DPDP compliance alone resolves the issue. Higher-risk flows, including data associated with Significant Data Fiduciaries, critical infrastructure or national-security sensitivities, warrant separate risk assessments and contingency planning.

Board oversight and documentation complete the architecture. Cross-border data exposure should be reported alongside other material business risks, while executed contracts, risk assessments, data maps and board records should be retrievable without reconstructing institutional memory under pressure. This approach reflects India's effort to balance cross-border digital commerce, innovation and regulatory sovereignty without relying on blanket data localization. In India's more permissive and innovation-oriented transfer model, digital trust depends less on keeping data permanently within national borders than on demonstrating where data goes, why it goes there and how the organisation remains able to control it.



About the Author

Dr. Sourabh V. C. Ubale

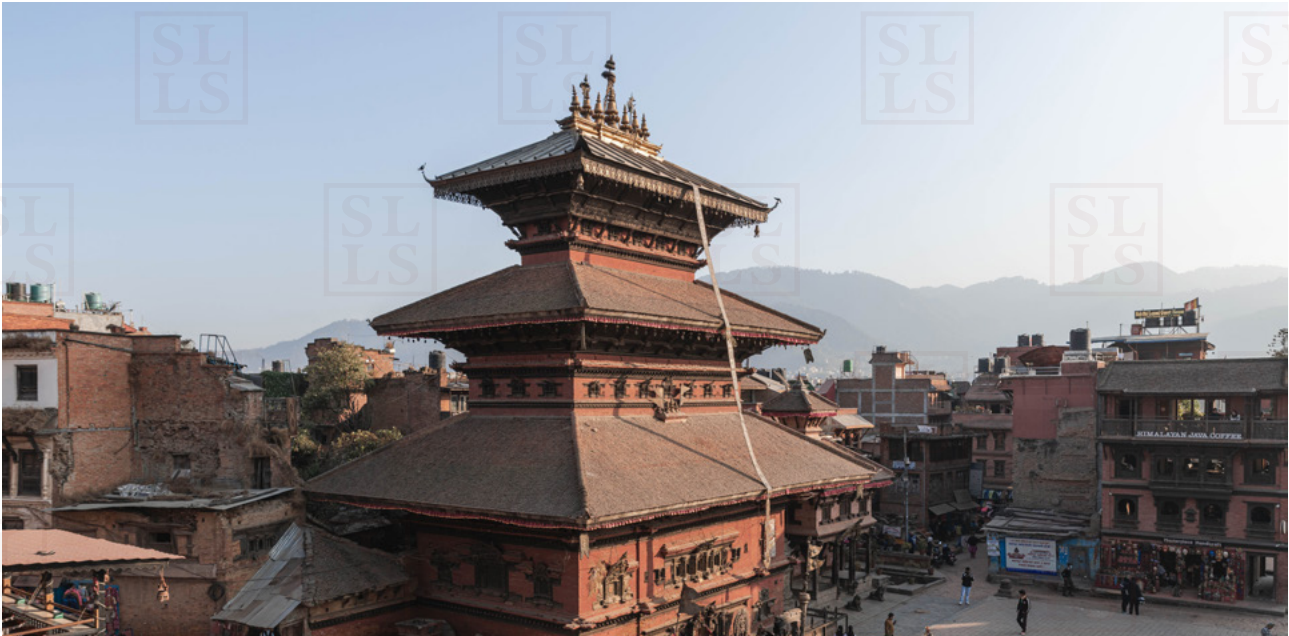
Assistant Professor (PG-Law), MM Shankarrao Chavan Law College, Savitribai Phule Pune University, Pune, Maharashtra, India

Dr. Sourabh Ubale holds qualifications in international law and advanced legal research, including an LL.M., Ph.D. and Post Doc. His academic interests include public and private international law, environmental and climate law, human rights, jurisprudence, and science- and technology-related legal issues.

Email: ubale.sourabh@gmail.com



Nepal - Governing AI and Data in Nepal Ahead of the Statute



Sector Focus: AI Governance · Data Protection · Cross-Border Data · Regulatory Readiness · Technology Disputes

Nepal's technology sector is being asked to demonstrate governance before its statutory framework is fully settled. For companies, investors and cross-border counterparties, the practical issue is therefore not simply what current law requires, but whether a business can already produce credible evidence of how it manages AI, data and technology risk.

Nepal's legal architecture remains fragmented. Article 28 of the Constitution protects privacy, while the Individual Privacy Act 2018 applies across public, private and not-for-profit bodies and criminalises unlawful collection or disclosure of personal information. The Electronic Transactions Act 2008 continues to govern cyber offences and digital signatures, supplemented by the Penal Code 2017 and sector-specific rules issued by Nepal Rastra Bank, the Nepal Telecommunications Authority and other regulators. Yet Nepal still has no statutory cross-border data-transfer regime and no independent data protection authority with dedicated audit or enforcement powers.

Institutional direction is nevertheless becoming clearer. In August 2025, the Government approved the National Artificial Intelligence Policy 2025, proposing an AI Regulation Council, a National AI Center, supporting national data and cloud infrastructure, Nepali-language datasets and a domestic-preference test for government AI procurement. The policy does not yet impose enforceable obligations on private companies, but it signals the direction of future governance. The Information Technology and Cybersecurity Bill 2025, meanwhile, is intended to replace the Electronic Transactions Act and would introduce measures including mandatory data destruction after defined retention periods, updated cybercrime provisions and a framework for cloud services and digital signatures.

For businesses, legislative gaps do not remove risk. Nepali technology companies already operate through overseas cloud hosting, outsourced development, regional payment systems and foreign investment structures. These relationships may import the expectations of foreign legal systems and counterparties even where Nepalese law is silent. Investors evaluating fintech, AI and platform businesses may therefore look beyond domestic minimum requirements and ask whether governance is documented, auditable and capable of supporting cross-border operations.

The practical response is to build that evidence contractually and procedurally now. Data-processing, cloud, outsourcing, shareholder and joint-venture agreements can specify storage location, retention and destruction periods, breach-notification timelines and audit rights. Where cross-border transfers are involved, contractual safeguards modelled on more developed privacy regimes may help demonstrate governability even where Nepal has no statutory transfer mechanism.

AI governance can follow the same approach. Companies need not wait for the proposed AI institutions before assigning senior-management responsibility for AI use-case review, model risk and human-oversight check-points. Incident-response protocols and contemporaneous records are equally important, particularly because existing criminal, contractual and tortious remedies remain available despite the absence of a dedicated data regulator.

Dispute design also matters. Technology licensing, joint-development and data-sharing agreements should consider institutional arbitration, confidentiality protections for technical evidence, interim relief for data or IP misuse, and clear choice-of-law provisions. In a period of regulatory transition, the company that can already show a functioning data framework, AI oversight process, incident record and dispute architecture is better positioned to respond when legislation eventually catches up with practice.

About the Author

Kumar Silwal

Advocate / Partner, Yaksha Law Firm · Kathmandu, Nepal

Kumar Silwal is a Kathmandu-based legal professional specialising in corporate and commercial law, taxation, dispute resolution, arbitration and regulatory compliance. He advises domestic and international clients on corporate transactions, foreign investment, contract drafting and tax litigation, with a practice focused on practical and commercially oriented legal solutions.

Email: kumar19silwal@gmail.com



Nepal - Emerging Markets - Aligning Cross-Border FinTech and Data Governance



Sector Focus: Cross-Border Fintech · Data Governance · Payment Infrastructure · AML/CFT · Regulatory Interoperability

Cross-border payment systems in emerging markets are scaling faster than the legal and governance frameworks that surround them. The central challenge is therefore not simply technical interoperability, but whether payment operators can prove compliance with data residency, privacy, capital controls, AML/CFT requirements and liability allocation before transaction volumes expand.

Three regional models illustrate the governance problem. The Nepal–India corridor links India’s Unified Payments Interface with Nepal’s National Payments Interface through NIPL and NCHL, supporting account-to-account transfers, merchant QR payments and increasingly digitised remittance flows. In Southeast Asia, Project Nexus and the ASEAN Payment Connectivity initiative pursue a multilateral model using a common gateway to connect domestic instant-payment systems. East Africa relies on the East African Payment System, linking national RTGS systems while mobile-money platforms integrate with regional banking networks.

The legal challenge is that interoperability crosses different data regimes. India’s Digital Personal Data Protection Act 2023, Nepal’s Individual Privacy Act 2018 and Privacy Rules 2022, and ASEAN’s Model Contractual Clauses approach cross-border processing differently. Central-bank requirements add another layer: the Reserve Bank of India’s 2018 payment-data storage directive and Nepal Rastra Bank IT Guidelines impose domestic data-residency expectations on payment operators. A workable response is a modular privacy architecture combining granular consent, data minimisation and tokenisation with a split-node database model: encrypted, short-lived transaction messages travel for real-time validation, while complete financial ledgers remain stored domestically for regulatory access.

Cross-border payment networks also require contractual clarity. Issuers, switches, acquirers and settlement banks should allocate responsibility for failed transactions, outages, fraud and API compromise through clearly defined service-level arrangements. Automated reversal mechanisms can prevent customer funds from remaining trapped across jurisdictions, while contractual allocation of cyber and fraud responsibility can reduce uncertainty when failures occur.

AML/CFT and capital controls need to operate at transaction speed. Real-time velocity and capping engines can enforce statutory transfer limits, API-based screening can check sanctions and politically exposed person lists before authorisation, and automated suspicious-transaction alerts can feed national financial intelligence units. The broader point is that retrospective compliance is poorly suited to instant payment infrastructure.

Implementation should therefore begin before commercial scale. Joint regulatory sandboxes can test settlement mechanics, cybersecurity and compliance controls in controlled environments. Technical infrastructure should support independent auditability through measures such as TLS 1.3, OAuth 2.0, zero-trust access and immutable logging. Operating agreements should combine joint governance mechanisms with binding international commercial arbitration, while rollout should proceed through constrained user groups, transaction limits and merchant categories before capacity is expanded.

The “Proof First” model ultimately rests on three forms of evidence: architectural proof, through privacy-by-design and split-node data structures; algorithmic proof, through automated AML, sanctions and capital-control mechanisms; and contractual proof, through clear allocation of liability across interconnected institutions. Standardised model clauses, joint regulatory sandboxes, harmonised dispute-resolution structures and more continuous supervisory technology could make those controls more portable across emerging-market payment corridors.

The practical lesson is straightforward: scalable digital finance depends not only on faster payment rails, but on governance that can travel with them.



About the Author

Erina Karki

Advocate / Partner, Agrani Law Associates · Nepal

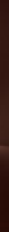
Erina Karki is a legal and taxation professional specializing in regulatory compliance, corporate governance, and cross-border financial frameworks.

Email: erina.karki17@gmail.com



Part V - Central Asia & Eurasia

Opening Note – From Digital Adoption to Proof-Based Governance



The modern world can no longer be imagined without electronic systems, digital tools, and artificial intelligence. To a greater or lesser extent, these technologies have become part of every sphere of human activity, including trade, healthcare, public administration, education, and many others.

This part of the journal examines selected aspects of digitalisation and the development of artificial intelligence in Central Asia and Eurasia. The region is rapidly introducing digital tools into corporate governance, financial markets, platform-based economies, and public administration. Yet the central question today is no longer simply how quickly digital services become available. Increasingly, companies, public authorities, and investors must be able to demonstrate that such services operate lawfully, securely, transparently, and fairly.

It is this transition - from digital adoption to proof-based governance - that connects the contributions in this section. Digitalisation creates new opportunities for shareholder participation, cross-border data transfers, the development of artificial intelligence, intellectual-property protection, and the scaling of platform business models. Yet these opportunities also bring a new level of responsibility. It is not enough to have electronic voting, cloud infrastructure, AI tools, or a digital platform. Organisations must be able to demonstrate how participants are identified, on what basis data are used, who supervises automated decisions, how assets are protected, and how digital evidence is preserved.

This issue is particularly significant for the countries of the region. They are developing amid active legal modernisation, growing international investment, and increasingly close connections with external markets. Uzbekistan illustrates how reforms in corporate governance, personal data, artificial intelligence, and digital intellectual property are gradually moving legal regulation from a formal framework into practical application. Kyrgyzstan demonstrates that cybersecurity and preparedness for dispute resolution depend directly on the quality of digital records and the ability to preserve evidence. The contributions concerning Türkiye and the United Arab Emirates broaden this regional perspective by showing that similar questions arise wherever technology, capital, and data cross multiple jurisdictions.

Central Asia and Eurasia deserve attention precisely because this transition is taking place here now - rapidly, unevenly, and with immediate practical significance. The region is not merely adopting digital technologies; it is seeking models that can make digital development understandable, verifiable, and worthy of trust. The materials collected in this section view this process as the emergence of a new culture of governance, in which technological opportunity must be accompanied by demonstrable responsibility.

Author: Dr. Kamola Batirova

Email: batirovakamola@gmail.com

Uzbekistan - Digital Corporate Governance and Investor Confidence: Lessons in Uzbekistan

Sector Focus: Digital Corporate Governance · Shareholder Rights · Investor Protection · Capital Markets · Electronic Voting

Uzbekistan's corporate governance reforms are increasingly using digital tools to improve shareholder participation and administrative efficiency. The central governance question is whether those tools can support equal, secure and legally reliable participation for both domestic and foreign investors.

Uzbekistan has made the development of an efficient and competitive securities market a priority, alongside reforms to corporate legislation, financing mechanisms and investor protection. Corporate governance is gradually being aligned with internationally recognised standards, while digitalisation has become an important part of making shareholder rights more accessible in practice.

A key change came in 2021, when amendments to the Law “On Joint-Stock Companies and Protection of Shareholders’ Rights” introduced remote participation in General Meetings of Shareholders. Information and communication technologies may now be used for participant registration, discussion of agenda items and electronic voting. Electronic document exchange with the Central Securities Depository has also replaced paper-based shareholder information in important areas, allowing companies to access registers through personal accounts and respond more quickly to corporate governance requirements. Remote meetings may be conducted through the e-vote.uz platform, which supports online participation, electronic ballots and shareholder identification.

These reforms have improved accessibility, but practical governance gaps remain. Shareholders must be notified of a forthcoming General Meeting at least twenty-one days in advance through several channels, including email, the Unified Corporate Information Portal, mass media and the company’s website, with additional publication requirements for listed companies. In practice, however, some shareholders do not provide email addresses to the Central Securities Depository. Where notice is not received for that reason, resolutions may still remain valid if other legal requirements have been satisfied. A possible improvement would be to require alternative notification through a registered address or phone number where electronic delivery is unavailable.

Foreign shareholders face a different challenge. Remote participation requires an electronic digital signature, relevant software, identification through the Unified Identification System and inclusion in the relevant shareholder registers. Uzbek citizens may obtain an electronic signature domestically or online, while foreign shareholders who are neither citizens nor physically present in Uzbekistan generally need to obtain one through Uzbek diplomatic or consular offices abroad. This can make remote participation slower and more burdensome. Allowing internationally recognised electronic identification or other reliable verification methods could reduce that friction while preserving cybersecurity controls.

Technical failures create another unresolved issue. Current legislation does not clearly address whether internet disruption, software malfunction or failure of the electronic voting system should postpone a meeting, invalidate a resolution or trigger an alternative voting process. There is also no established judicial practice on

such disputes. Until the law develops further, companies are encouraged to test electronic platforms before each meeting and document technical problems when they arise.

Uzbekistan's digital corporate governance reforms therefore represent meaningful progress, but investor confidence depends on more than digitisation itself. The next stage is to strengthen legal certainty around identity verification, technical failure and procedural safeguards so that remote participation is not only available, but genuinely effective and equal for all shareholders, including foreign investors.



About the Author

Dr. Kamola Batirova

Assistant Professor, Tashkent Metropolitan University; Partner, Liberator Law Firm · Uzbekistan

Dr. Kamola Batirova is a licensed advocate and company-law scholar whose work focuses on corporate governance, securities regulation, capital markets, investor protection and the legal dimensions of digital transformation. She holds a PhD in Law based on research into the regulation of IPOs in Uzbekistan and combines academic work with practical legal experience in corporate and commercial law.

Email: batirovakamola@gmail.com



Kazakhstan / AIFC - From Sandbox to Proof Infrastructure: Making Digital Finance, Tokenised Assets and Cross-Border Investment Governable

Sector Focus: Digital Finance · Tokenised Assets · FinTech Sandbox · Data Governance · Cross-Border Investment

The Astana International Financial Centre is developing from a special financial jurisdiction into a broader proof infrastructure for digital finance and cross-border investment. Its value lies in making legal perimeter, asset ownership, custody, data handling, cyber resilience and dispute resolution more legible to international capital.

AIFC operates under a special legal regime whose Acts may draw on principles, legislation and precedents of England and Wales and leading international financial centres. English is its official language, while the independent AIFC Court and International Arbitration Centre provide dedicated dispute-resolution mechanisms. Together, these institutions create a framework in which investors can assess governing law, regulatory authority and enforcement before committing capital.

The Astana Financial Services Authority is central to that architecture. Its FinTech Lab allows firms to test innovative financial and regulatory technology solutions with real clients under a simplified but supervised regime. The model is not regulatory exemption: applicants must demonstrate appropriate resources, AML/CFT arrangements and internal controls before progressing. The sandbox therefore creates evidence of what was tested, under which restrictions and with which safeguards.

The same proof logic is visible in digital assets. In June 2026, AFSA licensed Commodity Chain Ltd. to operate a tokenised real-world-asset platform in the agricultural sector through the FinTech Lab. The model links tokenised grain to physical assets using blockchain, IoT sensors, automated weighing and monitoring of storage conditions, illustrating how legal rights, asset verification, technical records and settlement mechanisms can be connected.

AIFC's Data Marketplace extends the approach to data commercialisation through licensing, privacy policies, terms of use and data-transfer agreements. Its growing links with Hong Kong exchanges also reinforce its cross-border investment role.

AIFC does not remove national-law, tax, sectoral, sanctions or physical-asset risks. Its significance is more disciplined: it provides structures through which those risks can be identified, tested and documented before scale. In the SLLS framework, AIFC demonstrates how Rules – Rails – Records – Readiness can convert innovation into investable proof.

About the Author
SLLS Global Research Team

Uzbekistan - Cross-Border Data Transfers under an Evolving Personal Data Legal Framework: A Jurisdictional Analysis of Uzbekistan



Sector Focus: Cross-Border Data · Data Localization · Privacy Compliance · Cloud & Payments · Regulatory Readiness

Uzbekistan has materially changed its approach to personal-data localization. The 2026 reforms replace a broad in-country storage obligation with a more targeted model, giving international businesses greater flexibility while preserving stricter treatment for defined categories of sensitive data.

Uzbekistan's Data Protection Law, originally adopted in 2019, was amended in 2021 to require personal data of Uzbek citizens processed through information technology to be collected, systematised and stored on servers physically located in Uzbekistan. Amendments introduced in March 2026 substantially narrow that rule. Mandatory localization now applies only to biometric data, genetic data and data relating to users of telecommunications operators operating in Uzbekistan.

Other personal data may be transferred abroad where one of three statutory mechanisms applies: transfer to a jurisdiction recognised as providing an equivalent level of protection; use of approved standard contractual clauses or binding corporate rules; or compliance with approved international standards for personal-data management and storage. This gives companies a clearer legal basis for structuring cross-border data flows, but the system remains only partly operational.

Resolution of the Cabinet of Ministers No. 415 of 29 July 2026 activates the adequacy route by recognising 49 states and territories as providing equivalent protection. The list includes most EU Member States, the United Kingdom, Switzerland, Japan and South Korea. Transfers to recognised jurisdictions through information systems established under international agreements may take place without additional permits or prior notification, provided measures are implemented to prevent leakage.

The other two statutory routes are not yet fully usable. Standard contractual clauses, binding corporate rules and international-standards mechanisms depend on requirements to be approved by the authorised state body, and those requirements had not yet been issued. Resolution 415 also leaves practical uncertainty around what qualifies as an "information system established under international agreements," with no detailed regulatory guidance yet available.

The reform also introduces concrete incident obligations. Where a leakage occurs during a cross-border transfer, the database owner or operator must notify the authorised state body within 24 hours and provide a detailed report on causes and remediation within 72 hours.

For global businesses, the immediate benefit is greater architectural flexibility, particularly for payment processors, digital wallets, cloud and SaaS providers, e-commerce marketplaces and multinational platforms that rely on centralised infrastructure. But the compliance burden has shifted rather than disappeared. Companies must now classify data correctly, identify which datasets remain subject to mandatory localization, and distinguish those that may move under the new transfer framework.

A practical compliance model starts with data mapping and classification, followed by confirmation of storage and processing locations. Businesses should prefer data-centre regions within recognised jurisdictions where appropriate, update consents and privacy notices to reflect cross-border processing, and maintain encryption, access controls, logging and incident-response procedures capable of meeting the 24/72-hour notification timetable.

The direction is clear: Uzbekistan is moving away from blanket localization toward a differentiated transfer regime. Greater freedom is available, but only where companies can demonstrate that classification, transparency, technical safeguards and transfer decisions are properly governed and documented.

About the Author

Saidaziz Alimov

Founding Partner, LEXCELL · Uzbekistan

Saidaziz Alimov advises on taxation and data privacy matters and contributes to the firm's work on complex cross-border regulatory and commercial issues affecting businesses operating in Uzbekistan. His clients include global tech giants, financial institutions, as well as multinational companies.

Email: saidaziz.alimov@lexcell.uz



Faringiz Karimova

Senior Associate, LEXCELL · Uzbekistan

Faringiz Karimova focuses on banking and finance and corporate matters, with experience relevant to businesses navigating financial, transactional and regulatory issues in Uzbekistan.

Email: faringiz.karimova@lexcell.uz



Umida Abduvakhobova

Junior Associate, LEXCELL · Uzbekistan

Umida Abduvakhobova works on corporate and data-protection matters, including issues arising from evolving personal-data and cross-border compliance requirements.

Email: umida.abduvaxobova@lexcell.uz



Uzbekistan - Building and Governing AI in Uzbekistan: Proving Data Compliance and IP Ownership Across the AI Lifecycle



Sector Focus: AI Governance · Personal Data · AI Training · IP Ownership · Trade Secrets

AI adoption in Uzbekistan is moving from experimentation into ordinary business use, but the legal risks arise across the entire lifecycle: data ingestion, model training, automated decision-making and commercial exploitation of outputs. The practical challenge is therefore to prove both lawful data use and defensible ownership of the resulting technology and content.

Uzbekistan's 2026 amendments to the Law "On Personal Data" confirm that AI training does not benefit from a special exemption. Personal data used for model development remains subject to ordinary requirements on lawful basis, purpose limitation, minimisation and security. Consent must be specific to the training purpose; contractual necessity may support processing integral to a disclosed service; and statistical or research use requires mandatory depersonalisation. Special-category, biometric and genetic data remain subject to stricter conditions.

Deployment creates a separate governance layer. The Law "On Informatization" prohibits AI-based information resources from harming life, health, freedom, honour, dignity or other inalienable rights, and legally significant decisions affecting rights and freedoms cannot rely exclusively on AI conclusions. The Data Protection Law similarly restricts solely automated decisions with legal or similarly significant effects. Credit scoring, insurance pricing and other high-impact uses therefore require meaningful human review, explanation and a route for challenge.

Liability has also increased. Law No. LRU-1115 of 21 January 2026 introduced elevated administrative penalties for unlawful personal-data processing using AI technologies, with repeat violations potentially escalating to criminal liability. The February 2026 AI Ethics Rules add soft-law expectations around fairness, non-discrimination, protection of restricted data and continuous human oversight.

Copyright creates a different uncertainty. Uzbekistan's copyright framework continues to define an author as a natural person whose creative labour created the work. Fully AI-generated output without meaningful human creative input therefore does not qualify for copyright protection. The 2026 reforms defined AI and strengthened the surrounding governance framework but did not change the human-authorship test.

For businesses, this creates an exclusivity risk. AI-generated marketing content, code, designs or other outputs may be commercially valuable yet unprotected if meaningful human contribution cannot be shown. The practical response is to maintain human-in-the-loop creative logs recording prompts, successive generations, edits, creative choices and final sign-off. Internal policies should distinguish between "AI-assisted" works, where human creative control can be demonstrated, and "AI-generated" works that should be treated as presumptively unprotectable. AI Solutions may not further rely to text-and-data mining exceptions and opt-out solutions afforded to them in foreign jurisdictions, and have to rely on clearly-expressed consents or licensing arrangements for works.

Not every AI asset depends on copyright. Human-authored application code and integration layers can remain conventional software assets. Model weights, fine-tuning datasets, prompt libraries and proprietary pipelines may be better protected through trade secret law where confidentiality and commercial value are preserved. Fully AI-generated outputs may require contractual restrictions, confidentiality and, where appropriate, trademark protection rather than an ownership claim that cannot be defended.

A practical AI governance file should therefore connect every system to its inputs, lawful data basis, copyright permission or exception, human review, output controls and asset classification. In Uzbekistan's developing AI ecosystem, the strongest position is not simply to use AI lawfully, but to maintain evidence showing why the data were usable, who exercised human judgment and which form of protection applies to each resulting asset.

About the Author

Saidaziz Alimov

Founding Partner, LEXCELL · Uzbekistan

Saidaziz Alimov advises on taxation and data privacy matters and contributes to the firm's work on complex cross-border regulatory and commercial issues affecting businesses operating in Uzbekistan.

Email: saidaziz.alimov@lexcell.uz



Sherzod Utkirkhujaev

Managing Partner, LEXCELL · Uzbekistan

Sherzod Utkirkhujaev focuses on the protection of intellectual property, brands, and businesses' digital assets in Uzbekistan. His clients include both international companies and globally recognised brands, as well as local businesses that require a systematic approach to rights protection and prompt action against infringements.

Email: u.sherzod@lexcell.uz



Sardor Inamov

Junior Associate, LEXCELL · Uzbekistan

Sardorbek Inamov's practice spans intellectual property transactions and disputes across various IP sectors, with experience in both prosecution, opposition and enforcement matters.

Email: s.inamov@lexcell.uz



Umida Abduvakhobova

Junior Associate, LEXCELL · Uzbekistan

Umida Abduvakhobova works on corporate, and data-protection matters, including issues arising from evolving personal-data and cross-border compliance requirements.

Email: umida.abduvakhobova@lexcell.uz



Uzbekistan - Digital IP Protection: Protecting Software, Digital Content and Brands



Sector Focus: Digital IP · Software Protection · Trademark Enforcement · Domain Names · Online Piracy

Uzbekistan has strengthened both the registration and enforcement side of digital intellectual property protection. For technology companies and international brand owners, the practical shift is toward faster formal registration, stronger sanctions and a greater need to preserve evidence of genuine use, ownership and infringement.

Two recent reforms are central. Law No. LRU-1080 of 8 August 2025 streamlined registration procedures and materially strengthened administrative and criminal sanctions for IP infringement. Software and database applications now undergo formal compliance review by the Intellectual Property Center under the Ministry of Justice, with approved rights entered automatically in the state register and electronic certificates issued with QR verification. The same reform expanded the Ministry of Justice's inspection powers and increased penalties for unauthorised use of trademarks, geographical indications, appellations of origin and firm names. Aggravated criminal cases can now result in fines or imprisonment of up to two or three years, including where infringement occurs through mass media or the internet.

Law No. LRU-1144 of 7 May 2026 addresses trademark "genuine use". Brand owners can no longer rely on the existence of a licence agreement alone to defend against a non-use cancellation action. They now need evidence of actual commercial use in Uzbekistan. This makes annual genuine-use audits increasingly important, particularly for international brands operating through local distributors or licensees. Relevant evidence may include dated packaging, invoices, local advertising, social-media activity, e-commerce listings and app-store use.

Digital enforcement remains more complicated. Uzbekistan does not recognise domain names as a separate object of exclusive right and has no dedicated administrative procedure equivalent to the UDRP for .uz disputes. Where a disputed domain incorporates a registered trademark, the rights holder generally needs to rely on conventional trademark infringement remedies through negotiation, administrative action or litigation. Defensive registration of .uz domains and realistic variants therefore remains one of the most cost-effective safeguards.

Software and app piracy create a different enforcement problem. Unauthorised redistribution of paid applications, cracked installers and pirated digital content may now fall within aggravated criminal provisions where infringement is committed online. Yet criminal enforcement still depends on financial thresholds and sufficient prima facie evidence, so rights holders should not rely on prosecution as their only remedy.

Formal registration can significantly strengthen the evidentiary position. Although copyright in software and databases arises automatically under the Berne Convention framework, Uzbekistan also offers dedicated state registration for computer programs and databases. For source code, algorithms and structured datasets, a QR-verifiable state certificate may provide stronger practical evidence before courts and inspectors than a general copyright deposition certificate.

Online enforcement also requires a two-track strategy. Uzbekistan has no IP-specific notice-and-takedown safe

harbour. Rights holders should first use the internal complaint tools of hosting platforms and social networks, while escalating recurring or locally based infringement through the digital regulators, the Ministry of Justice or, where appropriate, criminal channels. Platform removal alone may stop visibility without resolving the underlying infringement.

A sustainable 2026 digital IP programme should therefore combine formal software and database registration, genuine-use audits, defensive domain registrations and a standing enforcement playbook. The broader lesson is that registration is becoming easier, but meaningful protection increasingly depends on whether the rights holder can produce clear evidence of ownership, use and infringement when challenged.

About the Author

Sherzod Utkirkhujaev

Managing Partner, LEXCELL · Uzbekistan

Sherzod Utkirkhujaev focuses on the protection of intellectual property, brands, and businesses' digital assets in Uzbekistan. His clients include both international companies and globally recognised brands, as well as local businesses that require a systematic approach to rights protection and prompt action against infringements.

Email: u.sherzod@lexcell.uz



Maxim Park

Associate, LEXCELL · Uzbekistan

Maxim Park focuses on intellectual property transactions and disputes in the technology, automotive and telecommunications sectors, with experience in both prosecution and enforcement matters.

Email: maxim.park@lexcell.uz



Sardor Inamov

Junior Associate, LEXCELL · Uzbekistan

Sardorbek Inamov's practice spans intellectual property transactions and disputes across various IP sectors, with experience in both prosecution, opposition and enforcement matters.

Email: s.inamov@lexcell.uz



Uzbekistan / Central Asia - Navigating Platform Liability and Cross-Border Data Governance in Emerging TravelTech Ecosystems: A Boardroom Playbook from Central Asia



Sector Focus: Platform Governance · Cross-Border Data · TravelTech · Digital Commerce · Board Oversight

TravelTech platforms in Uzbekistan are moving from informal digital growth into a more demanding phase of operationally verifiable governance. The central issue for boards, investors and platform operators is no longer whether a digital business model is broadly permissible, but whether its transactions, data flows, merchant relationships and consumer interfaces generate evidence that can withstand regulatory, commercial and investment scrutiny.

Uzbekistan's 2025–2026 governance shift is being driven not by a single platform statute, but by the interaction of electronic commerce, tourism, licensing, taxation, personal data, cybersecurity and digital infrastructure rules. For online travel agencies, accommodation platforms and booking engines, legal classification increasingly follows the functions actually performed. A platform that collects payments, controls transaction terms or curates listings cannot rely solely on contractual language describing itself as a neutral technology intermediary.

Digital transactions are also becoming more traceable. Electronic commerce, banking, payment and tax systems increasingly require platforms to maintain auditable records of booking, payment, merchant settlement and fiscal reporting. For TravelTech operators, this means aligning customer-facing interfaces, payment gateways, internal ERP systems and fiscal records so that transaction timestamps, counterparties, commissions and tax-relevant values can be reconstructed when required.

Data governance has likewise moved beyond static privacy notices. Travel platforms process passport information, payment credentials, itineraries, geolocation and other sensitive information, requiring controls across collection, classification, access, encryption, cross-border transfer, retention and deletion. Uzbekistan's Personal Data Law and Cybersecurity Law provide the domestic baseline, while international standards such as GDPR accountability and privacy-by-design principles offer useful benchmarks for companies seeking cross-border scalability. The point is not to substitute foreign law for Uzbek requirements, but to build systems capable of demonstrating how those requirements are implemented in practice.

Electronic contracting creates another proof requirement. Platforms should be able to show which contractual terms, price disclosures and cancellation conditions were presented to a user at the moment of booking, how affirmative consent was captured, and how subsequent amendments, payments, complaints and refunds were recorded. In cross-border disputes, the evidentiary value of these digital records may be as important as the underlying terms themselves.

For boards, the broader risk is the accumulation of governance debt: unresolved weaknesses in merchant verification, platform classification, tax treatment, data controls, cybersecurity, contracts and dispute mechanisms that become more expensive when the company seeks institutional capital, enters M&A, or expands internationally. Such weaknesses may affect representations and warranties, indemnities, escrow arrangements, price

adjustments or closing conditions.

A scalable response is an Enterprise Proof Architecture linking statutory duty, internal governance, technical control, audit record and verifiable proof. That architecture should include proportionate merchant verification, contracts that match the platform's real economic role, lifecycle data controls, auditable digital consent, integrated complaint and dispute records, and crisis-ready cancellation, refund and continuity procedures. Board oversight should be risk-responsive rather than purely periodic, with material regulatory changes, cyber incidents, acquisitions or changes in data architecture triggering additional review.

For TravelTech businesses in Uzbekistan and Central Asia, the competitive advantage increasingly lies in being able to show not only that the platform works, but that its legal, technical and governance architecture can be explained, audited and trusted as it scales.



About the Author

Professor Liliya Ilkhomovna Achilova, DSc

Dean of the Master's Faculty, Academy of Justice of the Republic of Uzbekistan · Uzbekistan / Central Asia

Professor Liliya Achilova, DSc, serves as Dean of the Master's Faculty at the Academy of Justice of the Republic of Uzbekistan. Her academic and strategic advisory work focuses on business law modernization, corporate governance, digital economy regulation and cross-border platform accountability, with particular attention to legislative reform, judicial education and commercial dispute resolution across Central Asia.

Email: Liliya.achilova808@gmail.com



Kyrgyzstan/Central Asia - Proving Cybersecurity Governance in International Commercial Arbitration: Digital Evidence as a Tool for Protecting Technology Investments



Sector Focus: Cybersecurity Governance · Digital Evidence · International Arbitration · Technology Investment · Dispute Readiness

Cybersecurity governance is increasingly judged by evidence rather than policy language alone. In technology-related disputes, the ability to produce reliable logs, access records, forensic reports and incident documentation can determine whether a company can demonstrate responsible governance and protect the value of its digital assets.

Technology investments now depend not only on innovation, but on whether cybersecurity controls can be shown to operate effectively in practice. This matters particularly in cross-border relationships involving software, cloud infrastructure, artificial intelligence, digital platforms, trade secrets and technology licensing, where disputes frequently turn on what happened before, during and after a cyber incident.

Digital evidence has therefore become a governance asset. Audit trails, authentication records, access-control logs, forensic reports, incident-response files, backup verification and network-monitoring records can establish chronology, contractual compliance, security measures and the authenticity of electronically stored information. Their value extends beyond technical investigation: in arbitration, they may help demonstrate whether confidential information was adequately protected, whether cybersecurity obligations were fulfilled and whether the response to an incident was proportionate.

The absence of reliable evidence can create the opposite result. It may weaken a party's legal position, complicate fact-finding, increase procedural costs and make it harder to establish what controls actually existed. This is why forensic readiness should be treated as part of governance rather than as an emergency response after a breach. Organisations should define in advance how evidence will be collected, preserved and authenticated, including secure logging, access controls, chain-of-custody procedures and coordinated incident response.

International commercial arbitration can support that governance architecture. Technology disputes often involve source code, proprietary algorithms, AI models, customer databases, trade secrets and cybersecurity documentation. Arbitration can provide a forum for handling such technical and commercially sensitive material while allowing parties to structure procedures around confidentiality and expert evidence. But effective arbitration begins before a dispute: companies with established evidence-preservation processes and clear digital-record controls are better positioned when proceedings start.

Contract design is therefore part of cybersecurity governance. Agreements should address cybersecurity duties, incident notification, confidentiality, evidence preservation and cooperation during investigations. Dispute readiness can also be strengthened through periodic review of arbitration clauses, cybersecurity policies and evidence-management procedures so that contractual rights remain enforceable when a technology-related incident occurs.

Five practical disciplines follow. Cybersecurity should sit within board-level risk management with clear respon-

sibility and recurring oversight. Digital evidence should be generated, preserved and reviewed as part of normal operations. Contracts should allocate cyber responsibilities expressly. Forensic readiness should be established before incidents occur. Finally, dispute preparedness should be treated as a continuing governance function rather than a procedural issue considered only after a claim arises.

The broader point is that cybersecurity governance and arbitration are increasingly connected through proof. Companies capable of producing reliable, contemporaneous evidence are better positioned to protect technology investments, sustain investor confidence and resolve disputes efficiently across borders.



About the Author

Begaim M. Kaibyldeaeva

CEO, Business Soft LLC (Kyrgyzstan) & ICLOUD LLC (Uzbekistan, IT Park Resident) · Central Asia

Begaim M. Kaibyldeaeva is an Independent International Arbitrator and CEO of Business Soft in Kyrgyzstan and ICLOUD in Uzbekistan. She is a PhD Candidate at Tashkent State University of Law, where her research focuses on cybersecurity in international commercial arbitration. Her work spans arbitration, artificial intelligence, cybersecurity, digital evidence, technology governance and cross-border commercial law.

Email: begaimkaibyldeaeva@gmail.com



Turkey - The AI Shift in Arbitration: Efficiency Under Human Control



Sector Focus: AI in Arbitration · Cybersecurity · Professional Responsibility · Dispute Resolution · Legal Technology

Artificial intelligence is already changing how international arbitration is prepared, managed and argued. The opportunity is greater efficiency, but the governance challenge is equally clear: AI-assisted legal work still depends on human verification, professional responsibility and disciplined handling of sensitive case data.

AI tools are increasingly used by counsel and arbitrators for case management, document review, legal research, drafting and hearing preparation. In document-heavy technical disputes, they can materially reduce the time required to search, extract, compare and structure information. This does not remove the lawyer from the process. It shifts professional value toward strategy, judgment, asking the right questions and critically reviewing AI-generated outputs. The 2025 Queen Mary Survey, cited in the contribution, found that 91% of practitioners expect to use AI for legal research, reflecting how quickly these tools are becoming part of ordinary practice.

AI literacy therefore matters on both sides of a dispute. Lawyers need to understand how to prompt, test and verify AI tools, while businesses benefit from maintaining organised records and structured data that counsel can analyse efficiently when disputes arise. Better digital organisation before a dispute can directly improve the quality and speed of later case preparation.

The efficiency gains come with clear responsibility. AI may support calculations, financial models, evidence review, witness and expert work, or even legal arguments; but its outputs remain fallible. Recent cases in the United States and England involving non-existent authorities generated through AI demonstrate the risks of hallucination and over-reliance. Existing professional duties of competence and diligence continue to apply, making verification and fact-checking essential rather than optional.

Arbitral institutions are responding through governance, guidance and experimentation. CIArb, the SCC and the ICC have issued materials addressing confidentiality, accuracy and verification, disclosure and transparency, due process, human oversight and the limits of AI-assisted decision-making. The ICC has also established a dedicated Task Force on Artificial Intelligence in Dispute Resolution. In November 2025, AAA-ICDR launched an AI arbitrator for document-only construction disputes. Trained on more than 1,500 construction awards, the AI arbitrator generates draft awards for human review. The model remains explicitly “human in the loop”, reflecting continuing concern about delegating adjudicative judgment to AI. Questions surrounding enforcement of AI-assisted awards under the New York Convention also attract attention.

Cybersecurity is the other major governance issue. Arbitration files commonly contain trade secrets, financial information, privileged communications and business strategy. Uploading that material to AI tools may expose it to cloud storage in multiple jurisdictions with different data protection laws, third-party access, or reuse for model training. Legal teams therefore need to examine platform terms, data location, retention, encryption, access controls and deletion procedures before sensitive case material is processed.

For businesses, the practical implication is straightforward. They should expect counsel to use AI effectively, but also ask how outputs are verified, where data is stored, who may access it and whether providers may retain or reuse it. AI can improve arbitration, provided that efficiency gains are accompanied by appropriate human judgment, confidentiality safeguards and clear accountability.



About the Author

Misra Yalçın

Associate, Tahan | Cem Attorney Partnership · Istanbul, Türkiye

Misra Yalçın advises Turkish and international companies on complex commercial and large-scale construction matters and acts in arbitrations under ICC, LCIA, DIAC and ISTAC rules, as well as ad hoc proceedings. She also represents clients in arbitration-related court proceedings and serves as tribunal secretary in international arbitrations. She is admitted to the Istanbul Bar and holds an LL.M. in International Commercial Arbitration Law from Stockholm University.

Email: misrayalcin@tahan-cem.av.tr



Turkey - Audit Trails Are Not Enough: Building Proof-Bound AI Decisions for Scale



Türkiye - Audit Trails Are Not Enough: Building Proof-Bound AI Decisions for Cross-Border Scale

Sector Focus: AI Governance · Automated Decisions · Decision Evidence · Human Oversight · Cross-Border Compliance

For organizations using AI in consequential decisions, ordinary logs may show that a system produced an outcome without proving why that outcome was reached, which model and rules applied, or who had authority to approve or override it. For Türkiye-based and other non-EU companies whose AI outputs reach the European Union, that gap is becoming both a governance and market-access issue.

The EU AI Act can apply even where a company has no EU subsidiary, including where an AI system is placed on the EU market or its output is used in the Union. GDPR can likewise apply to controllers outside the EU that offer goods or services to, or monitor, individuals in the Union. The first governance task is therefore to determine scope, legal role and risk classification before deciding what evidence must be retained.

For high-risk AI systems, the AI Act requires automatic logging capabilities, effective human oversight and retention of relevant logs, while GDPR already requires accountability and imposes safeguards around certain significant automated decisions. The SCHUFA and Dun & Bradstreet Austria judgments further reinforce the need to explain how a particular automated outcome was reached. Yet these rules should not be overstated: they do not create a general obligation to reproduce every automated decision or prescribe a specific technology.

The author uses “proof-bound decision” as an analytical label, not a statutory term, for a decision record that links the relevant inputs, governing rules and model versions, the authority exercised and the final outcome. The recommended governance model is proportional: a product recommendation does not require the same evidentiary depth as a credit refusal, account closure or other consequential decision.

At decision level, several controls are particularly useful. Organizations should preserve the provenance and timing of inputs, because customer data, sanctions lists or financial information may change after the decision. They should record the specific model, policy, threshold and rule versions used, including externally supplied scores. The record should also show who was authorized to review or override the result, who actually acted, what that person saw, and whether the action ultimately executed matched the action approved. Where appropriate, the organization should support controlled replay or reconstruction and preserve the evidence in a tamper-evident form.

Supplier contracts are part of the same architecture. Deployers may need contractual rights to model-version identifiers, notice of material changes, relevant logs, retention support and cooperation in regulatory investigations. These controls also matter in transactions, where buyers may test whether historical AI decisions can be reconstructed from primary evidence.

We propose a four-stage compliance programme. Stage one — Scope and Ownership: identify consequential automated decisions, determine AI Act and GDPR applicability, assign legal roles and appoint accountable

executives. Stage two – Evidence Testing: attempt to reconstruct recent decisions and identify where the evidence chain breaks. Stage three – Control Design: define the minimum decision record, reconstruction standard, retention period, human-oversight process and supplier evidence rights. Stage four – Assurance and Reporting: repeat reconstruction tests after material changes and report results to the board based on evidence rather than policy attestations alone.

Evidence preservation should also form part of incident readiness: where a serious incident occurs, organizations should preserve the relevant system state and records before remediation changes make later reconstruction more difficult. Retention itself should remain proportionate, particularly where decision records contain personal or commercially sensitive information.



About the Author

Faruk Aktay, LL.M., Esq.

Managing Partner, Aktay Law Firm · Istanbul, Türkiye

Faruk Aktay is the Managing Partner of Aktay Law Firm and is qualified to practise in Istanbul, New York and England & Wales. He advises domestic and international clients on cross-border transactions, corporate and M&A matters, project finance, capital markets and regulated industries, and also acts in complex dispute-resolution and arbitration matters. He holds an LL.M. from New York University and has an academic background in both law and economics. He is also registered as a DIFC Courts Part II Legal Practitioner

Email: faruk@aktay.av.tr



Part VI - Africa

Sub-Saharan Africa - Governing the Digital Frontier: Data Protection, Cybersecurity and Responsible Technology Practice

Sector Focus: Data Protection · Cybersecurity · AI Governance · Board Oversight · Cross-Border Compliance

Digital governance across Africa is moving from formal compliance toward demonstrable accountability. South Africa, Nigeria and Kenya show three different enforcement paths, while South Africa's emerging AI policy and King V governance framework are pushing technology, data and cybersecurity more clearly into the boardroom.

South Africa provides the clearest anchor. The Protection of Personal Information Act (POPIA) has moved into active enforcement, including the Information Regulator's first R5 million fine against the Department of Justice and a settlement with WhatsApp concerning differences between protections afforded to South African and European users. Amendments to the POPIA Regulations on 17 April 2025 strengthened data-subject rights and direct-marketing requirements, while breach notifications have had to run through the Regulator's eServices portal since 1 April 2025. Unlike the GDPR, POPIA also carries criminal sanctions of up to ten years' imprisonment, reinforcing that data governance can involve personal as well as corporate exposure.

The regional comparison matters because similar legal templates have produced different enforcement styles. Nigeria's Data Protection Act 2023, supported by the General Application and Implementation Directive effective from 19 September 2025, has developed into a deterrence-led model. The Nigeria Data Protection Commission imposed a US\$220 million penalty on Meta and ₦766 million on MultiChoice, with major-controller penalties scaled to as much as 2% of annual gross revenue. Kenya has developed a more consent-focused body of regulatory practice: the Office of the Data Protection Commissioner has placed the burden of proving



consent on controllers and rejected implied or purpose-shifting consent, while the country has also opened the continent's first EU adequacy dialogue.

Cybersecurity is increasingly treated as a governance problem rather than an IT function. South Africa's experience, including the 2021 Transnet ransomware attack and earlier Postbank compromise, illustrates how weak institutional capacity can translate directly into operational disruption. Under POPIA, security safeguards, breach response and regulatory notification therefore require board-level visibility rather than being left solely to technical teams.

AI governance is developing through a different route. South Africa moved from its 2024 AI Policy Framework to a Draft National AI Policy published for comment in April 2026. At the same time, King V, published on 31 October 2025 and effective for financial years beginning on 1 January 2026, treats data, information, technology and AI as a distinct governance pillar. It calls for ethics, human-centricity, accountability, transparency, explainability, security, privacy, fairness and trustworthiness in AI use, with human oversight scaled to risk. Because King principles are cited by courts and incorporated into JSE listing expectations, corporate governance is already filling part of the space left by the absence of comprehensive AI legislation.

For businesses operating across Africa, there is no single continental compliance posture. South Africa, Nigeria and Kenya require separate treatment of transfers, enforcement exposure and governance evidence. Boards should therefore treat breach readiness, AI use-case mapping, King V alignment, cross-border transfer matrices, cyber capability and outsourcing dependencies as part of the same governance architecture. The practical test is whether the company can show how its systems are governed, how incidents are handled, and how local regulatory differences are managed before scrutiny arrives.

About the Author

Nicolene Schoeman-Louw

SchoemanLaw Inc · Republic of South Africa

Nicolene Schoeman-Louw is the Founder and Managing Director of SchoemanLaw Inc. She is an admitted Attorney of the High Court of South Africa, Conveyancer, Notary Public and Mediator, with experience advising entrepreneurs and businesses on corporate, commercial and governance matters. Her professional work also includes legal education, commentary and business-focused legal practice.

Email: nf.schoeman@schoemanlaw.co.za



Part VII- Latin America

Opening Note - Latin America in a New Era of Cross-Border Governance



Latin America has entered a period in which governance, regulation, and business transformation are increasingly shaped by global - rather than solely domestic - dynamics. As governments pursue growth, resilience, and competitiveness, the region is emerging as a critical testing ground for how international standards, investor expectations, and technological innovation converge in practice.

Across diverse markets, a common trend is taking hold: organizations are being asked to demonstrate not only compliance but credibility. Stakeholders expect evidence that corporate governance frameworks, sustainability commitments, data practices, and risk controls can deliver measurable outcomes. "Proof first" is no longer merely a regulatory expectation; it has become a strategic imperative.

At the same time, Latin America continues to attract international investment and remains deeply embedded in global trade, supply chains, and financial markets. That connectivity creates significant opportunities, yet it also exposes organizations to a complex web of cross-border obligations. Companies operating in the region must navigate evolving requirements that often originate beyond national borders - spanning transparency, sustainability, anti-corruption, data governance, and responsible business conduct.

The region's diversity enriches this landscape further. Although individual jurisdictions pursue distinct regulatory and economic priorities, many are converging around broader global governance themes. Latin America therefore offers valuable insights into how local implementation can coexist with - and reinforce - international standards.

The contributions that follow reflect this evolution. Drawing on perspectives from key Latin American markets, they illustrate how organizations are responding to heightened scrutiny, accelerating regulatory change, and rising stakeholder demands. Together, they highlight both the challenges and the opportunities facing businesses that seek to scale responsibly in a dynamic, interconnected environment.

As the global governance agenda continues to evolve, LATAM is not only adapting to change, it is helping define how effective governance frameworks translate into practical results across emerging and developed markets.

About the Author

Dr. José Francisco Mafla

Mr. Mafla is a Colombian attorney with broad experience in commercial law international business, M&A, customs and international trade. He serves as an arbitrator at the Bogotá Chamber of Commerce and formerly chaired Investment Committee of AMCHAM Colombia. He is ranked Band 2 by Chambers Latin America for International Trade/WTO, with more than 15 years of recognition, and recognised by Legal 500 as a Leading Individual, WWL as a Global Elite Thought Leader, LACCA as a top private practitioner in corporate practice.

Email: jmafla@bu.com.co



Brazil - Proving Governance in Brazil: A New Architecture for Technology, Data and AI

Sector Focus: Data Protection · AI Governance · Child Online Safety · Cross-Border Data · Regulatory Enforcement

Brazil's technology-governance environment has shifted sharply from formal compliance toward demonstrable accountability. An autonomous data-protection regulator, a new digital child-protection regime, an evolving AI framework and more structured cross-border transfer rules are collectively raising the standard of proof expected from companies operating in or reaching into Brazil.

A central change came on 25 February 2026, when Law No. 15,352/2026 elevated the National Data Protection Agency (ANPD) into a regulatory agency of special nature with functional, technical, administrative and financial autonomy. The restructured agency includes six superintendencies, one dedicated to technological innovation and management of the AI Regulatory Sandbox, and has expanded to roughly 500 staff. Its December 2025 Priority Topics Map for 2026–2027 also gives companies unusual visibility into future enforcement, with 75 planned actions focused on data-subject rights, children and adolescents online, public-sector processing, and AI and emerging technologies.

The second major development is the Digital Statute for Children and Adolescents, Law No. 15,211/2025, in force since 17 March 2026. The law applies not only to products designed for minors, but also to services “likely to be accessed” by children or adolescents, including social networks, marketplaces, streaming platforms, games and app stores, regardless of where the provider is headquartered. Obligations include stronger age-assurance measures, privacy-protective defaults, parental-supervision tools, restrictions on dark patterns and autoplay, and specific duties for generative AI systems interacting with minors. In August 2026, the ANPD used



the regime preventively to suspend a major messaging platform's live-streaming functionality until adequate safeguards for minors could be demonstrated.

Brazil's AI framework is also taking shape through two parallel tracks. Bill No. 2,338/2023, approved by the Senate in December 2024 and still under review in the Chamber of Deputies, would introduce a risk-tiered model with prohibited uses, high-risk impact assessments, human oversight and transparency duties. At the same time, the ANPD's AI Regulatory Sandbox is already testing governance practices in a supervised environment. Its July 2026 partial report identified gaps in governance, security, transparency and anonymisation, suggesting that regulatory expectations may harden through practice before the statute itself is enacted.

Cross-border data governance has also become more structured. Since 2024, ANPD rules have recognised standard contractual clauses, binding corporate rules and adequacy decisions, and in January 2026 the Agency issued its first mutual adequacy decision recognising the European Union.

For companies, the practical response is to build evidence rather than rely on policy statements. Sensitive data flows should be mapped; products should be assessed for child-access risk; AI systems should be inventoried and classified; and legal bases, impact assessments, age-verification logic, human oversight and remediation decisions should be documented when made. Because the ANPD now sits at the centre of data protection, child safety and emerging AI oversight, companies may also benefit from integrating privacy, trust-and-safety and AI-governance workstreams into a single governance architecture with a common evidence base.

About the Author

Laura Pontes Flores Lourenço

Senior Lawyer, FCAM – Ferraz e Camargo Advogados · Brazil

Laura Pontes Flores Lourenço is a Senior Lawyer at FCAM, specialising in Intellectual Property, Data Protection, Digital Law and Corporate Law. She advises domestic and international companies on privacy and data-protection projects, technology agreements, regulatory compliance, M&A, corporate reorganisations and due diligence across sectors including consumer goods, pharmaceuticals, automotive, civil aviation, energy, agribusiness and technology.

Email: LPLOURENCO@fcam.adv.br



Chile - Chile's Compliance Runway: Open Finance, Cybersecurity and Data Protection as Governance Evidence

Sector Focus: Open Finance · Data Protection · Cybersecurity · FinTech · Board Governance

Chile is entering a transition period in which open finance, data protection and cybersecurity are becoming parts of one operating governance system. The opportunity for companies is to use this implementation runway to build evidence before full regulatory pressure arrives.

Chile's Fintech Law, Law No. 21,521, created the Open Finance System, with the CMF issuing its initial framework in July 2024 and further technical amendments in June 2026. The system's operational start has been postponed to July 2027, but the delay is intended to support testing and phased implementation. Banks, fintechs and technology providers should therefore use the period to validate consent flows, API security, authentication, interoperability and customer-rights processes.

Data protection is developing in parallel. Law No. 21,719, published in December 2024, creates a new Personal Data Protection Agency and strengthens accountability for public- and private-sector processing. Although the Government proposed in September 2026 to postpone entry into force to December 2027, the direction is clear: companies will need more than privacy notices. Processing inventories, consent records, vendor controls, retention rules, breach procedures and transfer documentation will become increasingly important.

Cybersecurity obligations are already operational. Under Law No. 21,663, public and private entities providing essential services must report significant cyber incidents to the National Cybersecurity Agency (ANCI), with an initial report required within three hours of awareness. For payment, digital-infrastructure and financial-service providers, this requires pre-defined escalation, incident classification and coordination across legal, technical and operational teams.

The practical risk is fragmentation. A single fintech product may involve open-finance consent, personal-data processing, cloud vendors, AI analytics and cybersecurity reporting at the same time. Treating each issue in a separate file produces compliance fragments rather than governance evidence.

A stronger approach is a unified Chile governance pack covering open-finance role analysis, consent architecture, API testing, data inventories, privacy transition planning, cybersecurity classification, incident protocols, vendor oversight, AI use cases and board reporting. Chile's current runway should therefore be used to connect technical readiness with evidence that the company can explain, test and defend.

About the Author

SLLS Global Research Team

Mexico - Nearshoring Needs Proof: Data, Cybersecurity and Technology Governance for Mexico's Advanced-Manufacturing and Cloud Economy



Sector Focus: Nearshoring · Advanced Manufacturing · Cloud Infrastructure · Cybersecurity · Data Governance

Mexico's nearshoring opportunity is increasingly a technology-governance question. Moving production closer to North American markets also relocates data flows, industrial software, remote access, cloud dependencies, cybersecurity exposure and technology risk.

Modern Mexican manufacturing increasingly relies on robotics, sensors, ERP and MES systems, cloud analytics, AI-assisted quality control and remote vendors. The governance challenge is not that these systems are connected, but whether the company can explain who accesses them, where production and personal data are stored, how vendors connect, and what happens when a cyber incident disrupts operations.

Mexico's cloud infrastructure is also expanding, including AWS and Google Cloud regions in Querétaro. Local hosting, however, does not by itself resolve governance questions around overseas support access, backups, vendor sub-processing, industrial telemetry or AI use. Companies need a working data and infrastructure map rather than assumptions about location.

The 2025 Federal Law on the Protection of Personal Data Held by Private Parties strengthens the need for documented security measures, transfer controls, breach response and ARCO-rights processes. Fintech, payments and platform businesses must also account for sector-specific obligations, including local storage expectations for certain sensitive financial and payment data.

Cybersecurity remains fragmented at the statutory level, which makes internal governance more important rather than less. For advanced-manufacturing sites, IT and operational-technology risks should be governed together, with visibility over privileged access, vendor remote connections, backups, patching, incident escalation and recovery.

Contracts are the main control layer. Equipment, cloud, SaaS, AI and supplier agreements should address data location, remote access, cybersecurity, confidentiality, trade secrets, model-training rights, incident cooperation, downtime and exit support.

A practical Mexico governance evidence pack should therefore connect the operating model, industrial data inventory, personal-data compliance, cloud architecture, IT/OT controls, vendor access, AI use cases, technology contracts and board oversight. Nearshoring reduces distance; governable evidence reduces uncertainty.

About the Author

SLLS Global Research Team

Epilogue - Proof as the Condition for Scale



Technology, data and governance are no longer separate compliance disciplines. Across the jurisdictions examined in this edition, they increasingly converge around one operational question: can an organisation demonstrate that the systems on which its business depends are understood, controlled, documented and defensible when circumstances change?

The regulatory routes differ. Some jurisdictions rely on detailed statutory obligations and defined mechanisms; others depend more heavily on principles-based supervision, contracts, corporate governance or sector-specific controls. Yet the direction is increasingly consistent: governance is moving from policy statements toward evidence.

That evidence may take the form of data maps, AI registers, contractual controls, human-review records, incident logs, whistleblowing processes or board materials. The precise artefact varies, but the expectation is similar: responsibility should be capable of being located, reconstructed and tested.

This is the practical significance of the extended SLLS framework:

Rules – Rails – Records – Readiness – Results.

Rules establish the boundaries. Rails translate them into operating systems, contracts and responsibilities. Records preserve evidence that those mechanisms functioned. Readiness determines whether the organisation can respond when regulation shifts, systems fail, transactions are scrutinised or disputes arise. Results show whether governance continues to support credibility, investment, resilience and scale.

The objective is not regulatory uniformity. Different markets are developing different approaches to AI, data, cybersecurity, intellectual property, digital finance and platform risk. Effective cross-border governance therefore requires a stable enterprise core combined with jurisdiction-specific adaptation.

“Proof First, Scale Fast” is not an argument for slower innovation. It is an argument against scaling structures that cannot later explain themselves. Strong governance means knowing what matters, assigning responsibility clearly, preserving the right evidence and adapting without losing control.

That question leads directly into the next stage of the 2026 SLLS governance arc. **Q4 - TSR: Trade, Supply Chains and Resilience** - will examine whether these governance architectures remain effective when they move into the physical, contractual and operational networks through which cross-border business must continue under pressure.

The next test is no longer only whether governance can be proven, but whether it can remain resilient when the system itself is disrupted.



Disclaimer & Copyright Notice

This publication is for general informational purposes only and does not constitute legal, regulatory, investment, tax, technical, or other professional advice. It does not address the specific circumstances of any individual, organisation, transaction, or jurisdiction. No attorney–client, advisory, fiduciary, or other professional relationship is created by reading or using this publication. No solicitation or offer of services is intended.

Laws, regulations, standards, enforcement practices, and market conditions may change. The content is provided on an “as is” basis without warranties as to accuracy, completeness, timeliness, or continued applicability. Readers should obtain qualified professional advice before acting on any information contained herein. To the fullest extent permitted by law, SLLS Global and the contributors disclaim liability arising from reliance on this publication.

This publication may include forward-looking statements and references or links to third-party sources; such references do not imply endorsement. Trademarks are the property of their respective owners.

Views expressed in individual contributions are those of the respective contributors and do not necessarily represent the views of SLLS Global or other contributors.

© 2026 SLLS Global. All rights reserved.

This publication is a co-created knowledge product governed by the editorial and branding protocols of SLLS Global. Unauthorised reproduction, distribution, or commercial use is strictly prohibited without prior written consent.

SLLS Global is a non-commercial platform for collaborative knowledge creation. It is not a law firm, partnership, or unified service provider. Each contributor acts in their individual or institutional capacity. SLLS Global is not responsible for the independent views or professional activities of individual contributors. SLLS Global operates without separate legal personality and does not offer professional services to clients. The name “SLLS Global” reflects a shared intellectual and ethical commitment, not an integrated legal or commercial entity.

The SLLS name, logo, and publications are protected intellectual assets used under explicit licence or collaboration agreements governed by the SLLS Secretariat. This governance is administratively supported by SLLS Consulting Limited, an independent service provider designated to assist with operations. SLLS Consulting holds no ownership, decision-making rights, or editorial control over SLLS platform content or policy.

For permissions, licensing, or collaboration enquiries: contact@slls.global