

Foundation of Trust:

Data Strategies & Governance
in the Era of AI

A Report from The Praxellence Centre
Ltd online dialogue on July 10, 2026



Foundation of Trust:

Data Strategies & Governance in the Era of AI

A Report from The Praxellence Centre Ltd online
dialogue on July 10, 2026

Executive Summary

Praxellence held its first Dialogue on 10 July 2026, opening with a session titled "The Foundation of Trust: Data Strategies & Governance in the Era of AI." The session looked at how Singapore built the data foundations behind its digital government, and what that experience offers governments and organisations elsewhere navigating the same questions today.

Taken together, the individual pieces of this story point to one answer for why it worked. A clear mandate gave the effort authority to act across agencies that would otherwise have had no reason to cooperate. A single identifier gave Singapore's data infrastructure a common foundation to build on. And a clear legal mandate that held government to a harder standard than it asked of business gave the whole system its credibility. None of these, on their own, are technology decisions. Each is a decision about trust, made deliberately, well before any software was built.

"policy comes first, practice second, technology third."

That advice will only get more relevant. As AI moves from suggesting answers to acting on them, the same discipline that built Singapore's data foundation will decide whether the systems built on top of it can be trusted at all.

Background and session context

The dialogue's key speaker was Tan Kim Leng, an advisor with more than 35 years of experience in digital government, data governance and change management, whose work has spanned Singapore's public sector and international projects in countries including Rwanda, Vietnam, Tanzania, Mauritius and Fiji. By his own account, his involvement with Singapore's citizen data systems stretches back more than 35 years, to the early years of the government's shift into computerisation.

He set the tone early in the conversation: this was not a conversation about technology, but about how trust between government and citizens is built, and how easily it can be lost. That question of trust, earned deliberately and never assumed, runs through everything that follows, from the earliest policy decisions to the newest questions AI is raising today.

**Praxellence Founders at the first dialogue[WC1]*

Policy changes and data foundations

During the dialogue, Kim Leng argues that every digitalisation milestone that the country has achieved, from SingPass to daily-updated population data, can be attributed to policy decisions made in the late 1980's and revised over four decades since. This pattern has a clear direction: policy comes first, practice second, technology third.

"policy comes first, practice second, technology third."

The first solution was harmonising people data structures across the board. In the late 1980s, the nation introduced data standard for addresses in order to overcome inconsistent format, resulting in efficient mail delivery and citizen outreach. It was later adopted well beyond government, including across the private sector.

To strengthen the foundation so that future data will remain credible and reliable, two measures of accountability were set in place. Firstly, any changes to core data such as an address or a name, required a supporting legal documentation and recorded. Secondly, an agency became accountable only for the quality of its own data, not for the data coming from somewhere else. The latter requirement, he says, made agencies willing to share information.

Funding was also necessary for sharing. The Ministry of Finance of Singapore allocated funds for shared data infrastructure as a public good so that there could be no excuses for refusal due to budget constraints. These policy changes have built trust between the government and people of Singapore, allowing the nation to start progress into the right direction.

That single identifier now underpins Singpass, Singapore's national digital identity system, which today reaches 97% of the eligible population, according to the Ministry of Digital Development and Information.

Managing change and resistance

Resistance to projects like this rarely stems from technology, Kim Leng argued. People resist because they misunderstand the change, are misaligned with it, or sense their position or benefit is at risk. What they tell you is one thing; how they behave reveals the real concern. Read the behaviour, and you can design the right incentive instead of pushing harder.

That understanding shaped how the rollout itself was managed. Rather than trying to standardise everything at once, the effort began with a small set of roughly six core data fields, giving agencies running older legacy systems time to adapt against a fixed timeline.

Adoption was measured in nature as well. Successes were achieved for those who had agreed to adopt in advance and using their successes, they were able to persuade others into adoption.

The core obstacle, in Kim Leng's terms, was "departmentalism": agencies citing their own statutes as grounds to refuse shared standards. Breaking it took sustained leadership, not policy on paper. Governance failures share that root. When leadership weakens and departmentalism persists, governance cannot outlast a change in technology or administration.

Trust grew as discipline was upheld. Every time the team improved the system with demonstrable benefits, citizens trusted it more. When errors surfaced, the team disclosed them, fixed them, and let citizens' confidence recover. That is how Singapore sustained the system through decades of changing technology and changing leadership.

Establishing data standards and core registries

With data standardised, Singapore's next challenge was organising and processing it at scale. Kim Leng explained that the foundation work was laid out into three parts: the People Data Hub, the Business Data Hub and the Land Data Hub, each built and governed collectively so that no single effort tried to solve everything at once.

Four conditions made that possible, in his account: a mandate from senior government, backed by law where necessary; a working identification system for both people and organisations, Singapore's Unique Entity Number serving as the business-side equivalent of the personal ID; data standards that were enforced, not just published; and a strong commitment to share data across agencies, not merely collect it.

"Start with people data,"

Sequencing mattered as much as the conditions themselves. "Start with people data," he advises, because every other government service multiplies off it, and Singapore prioritised it accordingly. Business and land followed, land being the slowest and most complex given the added geospatial and ownership-mapping requirements on top of the registry itself. He frames this order specifically as advice for anyone trying to replicate the model, not just a description of Singapore's own history.

Once the three base registries were in place, Singapore extended the same approach into sector-level systems built on top of them, a pattern the next section covers in more detail.

The payoff shows up in measurable terms. Digital transactions built on this foundation are, on average, up to 80% faster than their pre-digital equivalents, according to government figures.

Ensuring privacy and data security

Kim Leng then expands to how Singapore handled privacy concerns and security of data. "Singapore runs two separate data protection laws rather than one," he explained, a public sector law governing how government handles citizen data, and a distinct law covering the private sector. Most countries, in his experience, cover both under a single law. He traces the split to history, where Singapore's data policies were originally built inside government, before any private-sector-facing law was enacted.

The split has caused Singapore to enforce accountability differently. A government officer who mishandles citizen data improperly can be held criminally liable, reflecting how much more severe the consequences of government error can be. Private companies instead face financial penalties, which he says can reach up to 10% of annual turnover. As he put it, the intent is to "hit their pockets" for companies, while making individual officers personally answerable in government, different levers of punishment aimed at the same underlying discipline.

A dialogue participant with a data privacy background added regional and global context. Malaysia introduced the first data protection law among ASEAN member states in 2010, with Singapore following two years later in 2012 and Thailand in 2021, placing Singapore among the region's earlier movers, though not the very first. He also pointed to the European Union's own enforcement record as a reminder of what's at stake when data protection fails at scale, citing the 1.2 billion euro fine issued against Meta in 2023 over unlawful data transfers, still the largest penalty ever handed down under the EU's GDPR.

The split matters beyond legal design. By holding government to a harder standard than it asks of business, Singapore's model puts the state's own credibility on the line first, before asking citizens or companies to trust it with their data.

Building trusted operating systems across industries

With the People, Business and Land data in place, Singapore extended the same discipline of standardising, mandating and sharing from managing data to transforming whole industries.

Starting with trade, the import-export activity generated considerable national income, so efficiency carried direct economic payoff. TradeNet built in 1990s', allows importers and exporters file declarations and move goods into Singapore quickly. The scale of that shift is well documented. Within its early years, TradeNet reduced permit approval, once a process taking 3 to 5 days, to under 10 minutes for 99% of applications, a benchmark Singapore Customs says the system still holds today. The old system has since evolved into a national trade platform carrying even more functionality.

Each sector followed the same governance sequence the registries did, created a sectoral data standard, build the system and bring everyone on board at a reasonable pace. Kim Leng calls the result a sectoral operating system and forthcoming case study will unpack these lessons, covering sectors from trade to construction.

The fragmentation that occurred among citizen information was replicated in business identity as the tax agency and the pension bureau each had their own business number. Now there is one agency responsible for issuing the UEN, the Unique Entity Number, which all other agencies use, and it has made everything quick and easy. GoBusiness, formerly known as LicenseOne or the online business licensing system, oversees the processing of licences and permits.

Governing AI with accountability

"AI is a probabilistic system, not a deterministic one"

One of the points brought up by Kim Leng was the potential role of AI in the quest for data strategies and governance. Kim Leng was direct that AI is a probabilistic system, not a deterministic one, meaning the same question can produce different answers on different days. That unpredictability, in his framing, is inherent to how AI works, not a bug to be patched out. It's also why data quality matters so much: an AI system is only as reliable as the data feeding it, and bad or outdated data doesn't just produce bad answers, it produces bad answers that sound confident.

Singapore's response has been to build testing into the system itself. The AI Verify Framework, developed by IMDA, checks systems across five dimensions before an organisation can call something "AI verified," and it's already used by the government, banks and telcos. Alongside that sits a firm human-in-the-loop requirement. His example was cause-of-death coding, where an AI system can suggest a code, but a human still has to approve it, keeping accountability for the decision with a person rather than "the system."

A question from the roundtable directed the conversation to whether institutions should prioritise clean data or staff AI literacy. Kim Leng's answer was to treat AI output like advice, not truth, weighing it the way you'd weigh advice from a person who has their own experience and blind spots. He warned that AI is "built and trained to please you," nudging users toward more engagement rather than necessarily more accuracy. His own habit, when uncertain about an answer, is to ask for a second opinion or a second AI system to check the first.

Conclusion and next steps

Taken together, the individual pieces of this story point to one answer for why it worked. A clear mandate gave the effort authority to act across agencies that would otherwise have had no reason to cooperate. A single identifier gave Singapore's data infrastructure a common foundation to build on. And a clear legal mandate that held government to a harder standard than it asked of business gave the whole system its credibility. None of these, on their own, are technology decisions. Each is a decision about trust, made deliberately, well before any software was built.

Kim Leng's closing advice to the room reflected that same order of operations. Rather than trying to fix everything at once, he suggested identifying the weakest link, whether that's a missing mandate, an unclear identifier, unenforced standards, or a reluctance to share, and starting there.

That advice will only get more relevant. As AI moves from suggesting answers to acting on them, the same discipline that built Singapore's data foundation will decide whether the systems built on top of it can be trusted at all.

About The Praxellence Centre Ltd

Advancing Public Sector Excellence through Impactful Digital Initiatives

The Praxellence Centre (Praxellence) operates as a not-for-profit organization dedicated to driving impactful digital initiatives across all layers of government. The name represents a deliberate fusion of two core principles: Praxis—the practical application of knowledge and skills—and Excellence—the state of superiority and merit. This philosophy guides the Centre's role as a strategic partner, assisting public sector institutions in navigating rapid technological shifts, rising citizen expectations, and complex socio-economic challenges.

While traditional consulting models often emphasize short-term recommendations, the mission here is to build deep institutional capacity. By providing governments with practical, evidence-based frameworks and robust implementation strategies, the Centre ensures technology serves as a permanent catalyst for public progress and governance excellence.

Strategic Support for Government Digital Initiatives

Four core pillars form the foundation for strengthening public institutions and delivering measurable impact:

- 1. Knowledge and Capacity Building:** Practical, practice-based training and capacity development programs are designed specifically to meet governmental and organizational outcomes.
- 2. Strategic Advisory:** Actionable, methodology-driven advice is offered to produce sustainable growth and measurable results for public initiatives.
- 3. Maturity and Readiness Assessment:** Public institutions are supported in

"Starting right" through specialized evaluations:

- a. Digital Government Preparedness**
- b. Data Governance Maturity Assessment (DGMA)**
- c. Change Readiness and Impact Assessment**

4. Thought Leadership and Discourse: High-level roundtables, seminars, and conferences are hosted to drive a positive narrative around digital outcomes and facilitate the exchange of global best Practices.

Bridging the Implementation Gap

The Praxcellence Centre aims to fill the critical gap between policy and outcome-driven strategy. By fostering collaborative ecosystems and delivering technology-enabled solutions, Praxellence aims to empowers the public sector to move beyond simple operational shifts toward long-term institutional development. The ultimate objective is to ensure digital transformation delivers genuine value to every citizen by leveraging technology's full potential within a framework of sustainable governance.

Contact information

The Praxellence Centre Ltd.
info@praxellence.org
www.praxellence.org