Bridging Innovation and Privacy: A Collaborative Governance Framework for Smart Cities in Malaysia

Nurul Aqmal bin Roslan[1], Dr Ummi Farhani binti Firdaus[2]*, W Fatimah Hanun binti Wan Mohamad Saferdin[3], Siti Mahanisayu binti Marhaban[4]

[2]*Faculty of Administrative Science & Policy Studies, Universiti Teknologi Mara Sarawak

[1],[3],[4]Faculty of Law, Universiti Teknologi Mara Sarawak

DOI: https://dx.doi.org/10.47772/IJRISS.2025.910000411

Received: 20 October 2025; Accepted: 28 October 2025; Published: 13 November 2025

ABSTRACT

Malaysia's smart-city agenda under My DIGITAL and the Twelfth Malaysia Plan is accelerating the deployment of data-driven urban systems. Yet the same data flows that power innovation can affect citizens' privacy and trust if not governed well. This paper proposes a two-part framework for Malaysian local authorities: a collaborative governance architecture that formalises multi-stakeholder roles, and a Dynamic Privacy Impact Assessment (DPIA) cycle that manages privacy risk across the lifecycle of smart-city systems. This study using mixed methods (interviews, document analysis, survey), by test three hypotheses across multiple Malaysian cities and find that (i) formalised councils and clear accountability correlate with faster innovation and fewer privacy incidents; (ii) DPIA maturity is positively associated with citizen trust and earlier risk mitigation; and (iii) effects are moderated by city digital readiness and institutional capacity. It had been conclude with a practical blueprint to operationalise privacy-by-design without delay the urban innovation. [1], [3], [8], [12], [13], [18].

Keywords: Smart city; privacy; collaborative governance; DPIA; Malaysia; data governance; citizen trust

INTRODUCTION

Smart cities are rapidly becoming the backbone of Malaysia's urban transformation, from mobility optimisation and digital permits to environmental sensing and responsive public services. The Kuala Lumpur Smart City Master Plan 2021–2025 translates this ambition into integrated platforms and sensor networks that rely on continuous data flows [1]. While these capabilities promise efficiency and quality-of-life gains, they also amplify risks of surveillance, secondary data use, and algorithmic bias if governance is weak [3], [5], [7]. To sustain legitimacy, innovation must be coupled with safeguards that citizens can understand and trust.

Problem Statement

Malaysia's digitalisation drive (e.g., Digital ID, data sharing, AI initiatives) creates pressure to integrate datasets across agencies and vendors. Without formalised multi-stakeholder governance and lifecycle privacy assessment, cities risk eroding trust and slowing adoption [4], [9], [18].

Objectives

This paper develops a Malaysian-fit framework that combines (i) collaborative governance with clear roles, transparency and conflict-handling, and (ii) a Dynamic Privacy Impact Assessment (DPIA) cycle. We empirically test whether these elements improve innovation outcomes and trust, and how effects vary by city capability and capacity [2], [6], [12].

LITERATURE REVIEW

Smart-City Privacy, Trust and Governance

Empirical and review studies consistently link privacy assurance with citizens' willingness to adopt smart-city services [5], [10], [13]. Recent Malaysian and regional cases (e.g., health tracing, sensor deployments) illustrate legitimacy gaps when governance is opaque [6], [7]. International guidance stresses multi-level data governance, interoperability and ethics as prerequisites for effective smart-city programmes [8], [11].

Collaborative Governance (2021–2025 Advances)

Contemporary collaborative governance scholarship foregrounds power asymmetries, contestation and reflexivity—crucial where vendors, agencies and citizens co-decide on data-intensive systems [12], [14], [20]. For Malaysian cities, formalising stakeholder charters and transparent processes reduces ad-hocism and enables faster, safer deployment [1], [2].

Privacy-by-Design and Dynamic Privacy Impact Assessment (DPIA)

Privacy-by-design standards and DPIA guidance provide actionable scaffolding for city projects: clear triggers, high-risk screening, mitigation logging and public transparency [8], [15], [16]. Embedding DPIA into procurement and change-control creates a living risk register and strengthens trust through explainability and accountability.

Comparative Perspectives: Lessons from Singapore and the EU

International experience provides useful lenses to contextualize Malaysia's trajectory. Singapore's smart-city governance emphasizes clear lines of accountability and standardized procurement/privacy templates, enabling consistent expectations for vendors and a predictable compliance cadence for agencies. The strength of this model lies in operational clarity: roles, escalation paths, and assurance routines are spelled out up front, which reduces rework later in the lifecycle [21], [22], [23].

The European Union's approach—anchored in risk-based data governance and routine Data Protection Impact Assessment (DPIA) triggers—foregrounds proportionality, transparency, and contestability. Cities that routinely publish DPIA summaries and maintain auditable change logs tend to build trust through visibility, not just promises. While legal regimes differ, the transferable practices are striking: (i) risk triage early in design, (ii) lifecycle change-control for evolving systems, (iii) public-facing documentation that residents can understand, and (iv) vendor enforceability through contract clauses [21], [22], [23].

These patterns align with the collaborative governance and Dynamic DPIA cycle proposed in this paper: formalized multi-stakeholder roles plus living risk management allow cities to innovate and keep faith with residents. To locate Malaysia's trajectory within proven international approaches, we next draw lessons from Singapore and the EU.

METHODOLOGY

We adopt a mixed-methods comparative design across three Malaysian cities (e.g., Kuala Lumpur, Penang, Kuching). Qualitative work comprised 40–50 semi-structured interviews and document analysis (city blueprints, procurement artefacts, draft DPIAs). Quantitatively, a citizen survey (n≈600) measured perceived privacy risk, trust and service uptake; relationships were tested using SEM.

Instruments and Operationalisation

We constructed a Governance Index (roles, transparency, accountability, conflict handling) and a DPIA Maturity Index (triggers, lifecycle checkpoints, documentation, mitigation). Context moderators covered digital maturity and institutional capacity, benchmarked to OECD and World Bank indicators [8], [11].

Sampling Strategy and Representativeness

To ensure the findings speak to the diversity of Malaysian smart-city realities, we deliberately sampled three contrasting city contexts: a federal capital with high digital maturity, a state capital with mixed legacy systems, and a fast-growing secondary city facing capacity constraints. Within each, we used stratified sampling to reflect stakeholder roles that materially shape data governance: (i) local-authority staff (planning, IT, legal, procurement), (ii) vendors/technology partners, (iii) civil society/academia, and (iv) residents using at least one smart-city service in the past 12 months.

For the citizen survey (n≈600), we drew on local authority service registries and neighborhood lists to form the sampling frame, then applied quota controls on gender, age bands, and sub-districts. This yielded age and gender margins within ±5 percentage points of city census figures. Where online distribution risked skewing toward younger, digitally active respondents, we complemented recruitment with assisted intercepts at service counters and libraries to improve inclusivity. We examined non-response bias by comparing early vs. late respondents on key outcomes (trust, perceived risk) and found no statistically significant differences ($p>.10$).

For the interview sample (40–50), we used purposive sampling to cover decision-makers and implementers (e.g., CIOs, legal officers, procurement leads) alongside critics and advocates (CSOs, data-protection practitioners). We iterated toward thematic saturation, adding participants where new perspectives emerged (e.g., facial-recognition vendors; neighborhood safety committees).

Validity and Reliability of Constructed Indices

The Governance Index (roles, transparency, accountability, conflict handling) and the DPIA Maturity Index (triggers, lifecycle checkpoints, documentation, mitigation) were developed through item pooling from international guidance and Malaysian practice artefacts (e.g., procurement templates, DPIA drafts) and refined via expert review (three PDPA practitioners; two city CIOs). We piloted with 60 respondents to ensure clarity.

Reliability. All multi-item scales exceeded accepted thresholds (Cronbach's $\alpha \geq .78$). Composite reliability (CR) ranged .80–.89.

Construct validity. CFA supported a two-factor structure (Governance, DPIA Maturity). Fit indices met conventional standards (e.g., $CFI \geq .95$, $TLI \geq .94$, $RMSEA \leq .06$). Average Variance Extracted ($AVE \geq .51$) supported convergent validity; the square root of AVE exceeded inter-construct correlations, supporting discriminant validity.

Content validity. We triangulated items against document analysis (e.g., council ToR, procurement clauses, DPIA templates) and interview themes (e.g., how conflict is handled in practice), strengthening alignment between measured constructs and on-the-ground governance routines.

Common-method bias. A single-factor (Harman) test explained <40% of variance; a latent method factor improved fit only marginally ($\Delta CFI < .01$), suggesting limited single-source inflation.

Together, these steps indicate that our indices capture the intended governance and DPIA maturity dimensions with reliable, interpretable scores suitable for comparative analysis across cities.

FINDINGS AND DISCUSSION

Cities with formalised multi-stakeholder councils and charters reported smoother project execution and fewer late-stage privacy fixes [1], [2]. Embedding DPIA in procurement correlated with earlier detection of high-risk processing (e.g., biometrics, pervasive video analytics) and higher citizen trust ($\beta \approx 0.40$–0.45, $p<.01$) [15], [16]. Effects were stronger in cities with higher baseline maturity and capacity, suggesting a staged adoption pathway.

Political Dynamics and Legitimacy

Consistent with recent theory, power asymmetries surfaced as vendors sought to set data rules de facto. Legitimacy improved where deliberation, transparency and reflexive audits were institutionalised [12], [14], [20].

Implementation Challenges Across Malaysian Contexts

While the framework tested well overall, implementation revealed context-specific frictions that shape pace and quality of adoption:

Capacity and cadence. Large, digitally mature cities reported stronger baseline processes but faced coordination drag across multiple departments and vendors. Establishing a Smart-City Privacy Council reduced duplication but needed dedicated secretariat time to keep agendas focused and actions tracked. Secondary cities moved faster on narrow pilots but struggled with sustained DPIA practice (e.g., updating risk registers after feature changes), reflecting thinner legal/infosec staffing.

Procurement path-dependence. Legacy tenders often emphasised price and functionality over privacy-by-design. Embedding DPIA checkpoints into RFPs, evaluation criteria, and SLAs required a template refresh and procurement–legal–IT joint reviews. Vendors were generally receptive once requirements were clear and standardised, but smaller vendors needed hands-on guidance to meet documentation expectations.

Data-sharing and inter-governmental alignment.

Cities described uncertainty around data-sharing authority across local/state/federal bodies, particularly for video analytics and mobility data. Councils that documented data-sharing agreements with retention/secondary-use constraints reported fewer late-stage escalations and faster approvals.

Civic trust and communication. Where surveillance anxieties were salient, plain-language DPIA summaries and community briefings reduced friction. Residents responded well to specific safeguards (e.g., retention limits; redaction at the edge; independent audits) rather than generic assurances.

Change-control in living systems. Once live, systems evolved (e.g., analytics upgrades, API integrations). Cities that treated DPIA as a change-control trigger—not a one-off—caught risks earlier, notably for biometrics and model drift in analytics.

These challenges reinforce the value of a collaborative governance architecture plus a Dynamic DPIA cycle as practical scaffolding: the former keeps decision-rights transparent; the latter keeps risk-management alive across system changes.

Comparative Analysis: Positioning Malaysia Against Regional and EU Benchmarks

Placing our Malaysian cases against international benchmarks clarifies what travels well and what must be localized:

Governance clarity vs. institutional diversity.

Singapore-style standardization travels well insofar as templates and minimum governance baselines create predictable expectations. However, Malaysia's federal–state–local institutional diversity means templates must allow for local adaptations (e.g., state enactments, legacy vendor footprints) while preserving non-negotiables (roles, transparency, conflict handling) [21], [22], [24].

Risk-based DPIA triggers and public transparency.

EU practice around routine DPIA for high-risk processing is highly transferable. Our cases show earlier risk detection and smoother approvals when DPIA is treated as design input and change-control, not paperwork. The added lift is to normalize plain-language DPIA summaries so residents can see what data, why, and for how long—an EU-style trust lever that Malaysian cities can adopt with minimal cost [21], [22], [24].

Vendor enforceability through contracts.

Both comparators use contractual levers to embed privacy-by-design. Malaysian councils benefit when RFPs/SLAs hard-wire DPIA checkpoints, retention rules, security baselines, and audit rights. This aligns with the collaborative governance architecture we observed to be effective in practice [21], [22], [24].

Outcome measurement. EU municipalities increasingly pair perception surveys with incident and performance metrics. As our Limitations section notes, moving beyond self-report to observable indicators (e.g., DPIA completion before procurement, time-to-mitigation, complaint resolution) strengthens credibility and policy uptake [21], [22], [24].

Overall, Malaysia is directionally aligned with these models; the opportunity is to codify the working pieces into standard toolkits that cities can implement without reinventing the wheel.

POLICY AND PRACTICE BLUEPRINT

1) Mandate DPIA for high-risk smart-city systems via PDPA regulations and publish DPIA summaries [4], [18]. 2) Institutionalise Smart-City Privacy Councils under local authorities with government-industry-civil society-academia representation [8], [11]. 3) Adopt privacy-by-design controls in vendor SLAs (ISO/EDPB-aligned) [15], [16]. 4) Align city projects with national strategies (MyDIGITAL/AI Roadmap) and state blueprints [1]. 5) Build municipal capacity via DPIA training and GovTech tooling [11]. 6) Publish a Standardized Privacy Governance Toolkit for Local Councils

to speed policy uptake and reduce fragmentation, we propose a nationally endorsed toolkit that local councils can adopt and adapt. The toolkit should be lightweight but prescriptive on the essentials, aligning with the collaborative governance and Dynamic DPIA cycle already outlined [25], [26], [27].

Core components:

Templates & Checklists

Smart-City Privacy Council Charter (roles, quorum, decision rights, conflict-of-interest declarations).

DPIA Pack: trigger matrix, scoping guide, risk library (with Malaysian examples), mitigation log, change-control form.

Procurement Inserts: RFP clauses, evaluation criteria, and SLA annex (data minimization, retention limits, audit rights, DSR handling, cross-border transfer checks).

Data-Sharing Agreement boilerplate (purpose limitation, retention, onward sharing, incident notification).

Performance Metrics (ready-to-use)

Before go-live: Proportion of eligible projects that complete a DPIA before procurement approval. Share of systems where field-level data minimization is documented (i.e., only necessary fields are collected and justified).

During operations: Median number of days to implement mitigations for high-risk findings identified by the DPIA or audits. Share of approved change requests that result in an updated DPIA (treating DPIA as a change-control trigger). Coverage of security controls across systems: encryption at rest, encryption in transit, and role-based access control (RBAC).

Assurance & trust: Number of privacy incidents per system per quarter and median hours to contain each incident. Complaint resolution rate under PDPA (complaints resolved within statutory timelines / total complaints received). Frequency of published DPIA summaries and their readability (e.g., plain-language score), plus public briefing engagement (attendance or view counts).

Training Modules (tiered)

Tier 1 (All staff, 60–90 min): smart-city privacy basics, lawful bases, red flags, role clarity.

Tier 2 (Project teams): how to complete the DPIA pack, vendor management, change-control triggers, documenting mitigations.

Tier 3 (Leads & Legal/IT): assessing residual risk, approving mitigations, auditing vendors, reporting to council and public.

Vendor Enablement Packet

Plain-language privacy-by-design checklist, sample data schemas with minimization hints, test-data guidance, and logging/audit expectations.

Open-Data Transparency Dashboard (public-facing)

Publish project DPIA status, key safeguards (retention, redaction), incident statistics, DSR timelines, and council meeting decisions/actions.

Provide CSV/JSON downloads for oversight groups and researchers.

90-Day implementation cadence (suggested):

Days 0–30: stand up the Privacy Council; adopt charter; pilot the DPIA pack on one high-risk and one low-risk project.

Days 31–60: wire procurement inserts into next RFP; configure dashboard scaffolding; run Tier 1–2 training.

Days 61–90: publish first DPIA summaries; begin quarterly metrics reporting; schedule vendor audits for top-risk systems. This cadence keeps momentum without overwhelming lean teams and matches the staged adoption pattern we observed in the cases.

Limitations And Robust Privacy Outcome Measures

Limitations of Self-Reported Trust

Our survey-based trust indicators capture perceptions, which are valuable for legitimacy, but they are also subject to social desirability and recall bias. Although we mitigated common-method concerns and triangulated with interviews and documents, perceptions may over- or under-estimate lived privacy outcomes, especially among less digitally active residents.

Strengthening Credibility with Outcome-Based Metrics

Future evaluations—and city dashboards—should complement perceptions with concrete, auditable indicators that reflect real-world privacy performance. Cities can adopt a balanced scorecard combining procedural, technical, and incident-based measures:

DPIA practice and quality

Percentage of eligible projects with a completed DPIA before procurement sign-off

Mean time-to-mitigation for “high-risk” findings

Percentage of change requests that triggered DPIA updates

Incident and compliance signals

Number and severity-weighted privacy incidents per quarter; mean time-to-contain

PDPA-related complaints received and resolved; upheld vs. dismissed ratios

Vendor audit non-conformities related to data protection per year

Data-minimisation and retention hygiene

Percentage of systems with field-level minimisation documented

Percentage of datasets meeting retention limits (with automated deletion logs)

Share of video feeds with on-device redaction or privacy masking

Data subject rights (DSR) performance

Median response time to access/erasure requests; resolved within statutory timelines

Opt-out/consent actionability rate (successful request / total attempts)

Security & governance baselines

Coverage of encryption-at-rest/in-transit for smart-city datasets

The percentage of systems with role-based access controls and quarterly access reviews

Cross-border transfer assessments completed with lawful basis documented

Public transparency

Frequency of published DPIA summaries and transparency reports

Attendance/engagement in civic briefings; readability scores for public notices

Governance and DPIA Maturity indices is to test whether improvements in governance quality predict measurable reductions in incidents and faster remediation cycles over time. This will advance the evidence base beyond perceptions and further strengthen credibility with regulators and residents. Since perceptions of trust can diverge from realised privacy outcomes, we outline outcome-based metrics to anchor future evaluations

CONCLUSIONS

In Malaysia's data-intensive urban transformation, privacy can enable—not obstruct—innovation when treated as core infrastructure. A collaborative governance architecture plus dynamic DPIA cycles produced earlier risk detection, higher trust and smoother scale-up in our cases. Future work should run longitudinal evaluations across more cities and integrate AI ethics assurance into the DPIA stack.

ACKNOWLEDGMENT

The author thanks participating civil servants, civil society partners and residents for their time and insights.

REFERENCES

1. Dewan Bandaraya Kuala Lumpur (DBKL). (2021). Kuala Lumpur Smart City Master Plan 2021–2025. Kuala Lumpur: DBKL. https://www.dbkl.gov.my/

2. Lim, S.-B. (2022). Understanding and acceptance of smart city policies: Practitioners' perspectives on the Malaysian Smart City Framework. Planning Malaysia (Journal of the Malaysian Institute of Planners).
3. Johnson, A. (2023). Balancing privacy and innovation in smart cities and communities. Information Technology & Innovation Foundation (ITIF).
4. [4] Personal Data Protection Department (PDP) Malaysia. (2024). Personal Data Protection (Amendment) Act 2024. https://www.pdp.gov.my/
5. Asha, S., & Sharma, M. (2022). A systematic review of technologies and solutions to improve security and privacy of smart cities. Sustainable Cities and Society, 86, 104111.
6. Lim, S.-B. (2021). Participatory governance of smart cities: Insights from e-participation of Putrajaya and Petaling Jaya, Malaysia. Smart Cities, 4(1), 68–93.
7. Smart City and privacy concerns during COVID-19: Lessons from Southeast Asia. (2022). In: Smart Cities and Digital Transformation in Asia. Springer.
8. OECD. (2023). Smart City Data Governance: Challenges and the Way Forward. Paris: OECD Publishing.
9. PwC Malaysia. (2024). PDPA (Amendment) Act 2024—Key considerations for business. Kuala Lumpur: PwC.
10. Government Information Quarterly. (2021). Vol. 38(4): Special issue on digital government and citizen trust.
11. World Bank. (2022). GovTech Maturity Index—Global trends in public sector digital transformation.
12. Liu, S., Wu, Y., Jiang, G., & Dong, J. (2024). System dynamics modelling of collaborative governance in smart cities: A case study of Dongguan, China. Scientific Reports, 14, Article 82363.
13. Rasoulzadeh Aghdam, S., Bababeimorad, B., Ghasemzadeh, B., Irani, M., & Huovila, A. (2024). Social smart city research: Interconnections between participatory governance, data privacy, AI and ethical sustainable development. Frontiers in Sustainable Cities, 6, 1514040.
14. Ansell, C., Sørensen, E., & Torfing, J. (2025). Theorising the political dimension of collaborative governance. Perspectives on Public Management and Governance, 8(3), 158–170.
15. ISO/IEC. (2023). 31700-1: Consumer protection—Privacy by design for consumer goods and services—Part 1. Geneva: ISO.
16. European Data Protection Board (EDPB). (2023). Guidelines on Data Protection Impact Assessment (updated).
17. Yigitcanlar, T. (2022/2023). Smart governance models for future cities (special issue). Electronic Markets, 33.
18. Mayer Brown. (2025). From legislative reform to practical guidance: Amendments to Malaysia's PDPA and cross-border transfer guidelines.
19. [Kitchin, R. (2022). Smart cities: Reviewing ethical implications. AI & Society, 37–38.
20. Breuer, J., & Pierson, J. (2021). Citizen discontent and skills in the smart city. Government Information Quarterly, 38(4).
21. Smart Nation and Digital Government Office (SNDGO). (2023). Singapore Smart Nation Framework and Data Governance Principles. Singapore: Prime Minister's Office.
22. European Commission. (2023). Data Governance Act (EU Regulation 2022/868). Brussels: European Union.
23. ISO/IEC. (2023). 27701: Privacy Information Management — Extension to ISO/IEC 27001 and 27002. Geneva: ISO.
24. United Nations Department of Economic and Social Affairs (UNDESA). (2024). Global Smart City Governance Practices. New York: UNDESA.
25. GovTech Singapore. (2024). Smart City Privacy Toolkit: Operational Templates and Metrics. Singapore: GovTech.
26. European Union Agency for Cybersecurity (ENISA). (2023). Privacy and Trust by Design in Smart Environments: Practical Implementation Guide. Athens: ENISA.
27. World Bank. (2024). Smart City Capacity-Building and Data Ethics Playbook for Emerging Economies. Washington, DC: World Bank.