

Substance Without Formality: Personal Data Protection Governance in Yogyakarta City, Indonesia

Ismail Nurdin¹, Ikra Novar Rizqi², Ari Apriyansa³, Sri Hartati⁴

¹Institut Pemerintahan Dalam Negeri, ismailnurdin@ipdn.ac.id

²Institut Pemerintahan Dalam Negeri, ikra@ipdn.ac.id

³Institut Pemerintahan Dalam Negeri, ari.apriyansa@ipdn.ac.id

³Institut Pemerintahan Dalam Negeri, sri_hartati@ipdn.ac.id

HOW TO CITE: | ABSTRACT:

Ismail Nurdin, Ikra Novar Rizqi, Ari Apriyansa, Sri Hartati (2026). Substance Without Formality: Personal Data Protection Governance in Yogyakarta City, Indonesia International Journal of Special Education, 41(23s), 435-457

Indonesia's Personal Data Protection Law (Law No. 27/2022) obligates local governments to act as accountable Data Controllers, yet its two-year transition period expired in October 2024 without the mandated national supervisory authority (Data Protection Agency, or Badan PDP) being established, and without any of the nine implementing government regulations the Law requires. This single-case study examines how personal data protection (PDP) governance is constructed in Yogyakarta City, a municipality embedded in Indonesia's only constitutionally privileged regional autonomy regime, the Special Region of Yogyakarta (Daerah Istimewa Yogyakarta, DIY). Primary data were drawn from one multi-stakeholder focus group discussion with fourteen informants spanning government, academia, the press, industry, and citizens, analyzed through thematic analysis and interpreted through four complementary lenses: institutional theory, street-level bureaucracy, collaborative governance, and the political economy of bureaucracy. To strengthen a single-case design, the primary findings are triangulated against two forms of secondary comparative analysis: an international benchmarking of five data-protection regimes (the European Union, Singapore, Malaysia, China, and Thailand) and a domestic comparison with three other Indonesian local governments (Surakarta, Pekalongan, and Bantul Regency). Findings reveal a consistent pattern across all levels of analysis: substantive-partial compliance without complete formal structure, an inversion of the ceremonial-without-substance pattern that dominates institutional compliance literature. A twelve-indicator maturity assessment shows the gap is concentrated in four specific structural indicators (a formally designated Data Protection Officer, a data-

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.

Open access publication under the terms and conditions

of the Creative Commons Attribution (CC BY)

license (<http://creativecommons.org/licenses/by/4.0/>).

breach notification procedure, a dedicated PDP budget line, and formal coordination with the DIY provincial government) rather than distributed evenly across the governance system. The study proposes a six-component Adaptive PDP Governance Model with an indicative quarterly roadmap and offers practical implications for Indonesia's Ministry of Home Affairs and local governments sharing similar institutional characteristics.

Keywords- institutional, collaborative, established, discussion

Introduction

1.1 Background and Context

Digital government transformation has repositioned personal data as both a strategic public asset and a locus of institutional vulnerability (Mergel, Edelmann, & Haug, 2019; Vial, 2019). As governments digitize citizen services, accountability for the data those services generate has shifted from a technical concern into a central governance problem (Gao, Sun, & Wang, 2023; Jin & Wang, 2025). Indonesia's legislative response, Law No. 27 of 2022 concerning Personal Data Protection (hereafter, the PDP Law), obligates every Data Controller and Data Processor — including central and local government agencies — to meet binding standards of lawful processing, informed consent, data security, and breach notification. The Law's two-year transition period, mandated under Article 74, expired in October 2024. By 2026, when this study was conducted, any governance gap at the local level therefore carries direct legal consequence rather than merely anticipatory risk.

1.2 The National Institutional Vacuum

Despite the transition period's expiry, the PDP Law's institutional foundation remains incomplete at the national level. The independent supervisory authority mandated under Article 58 (the Data Protection Agency, or Badan PDP) had, as of this study, still not been formally established. At least nine implementing government regulations envisioned by the Law — covering data processing procedures, data protection impact assessment, compensation procedures, data-subject rights procedures, and corporate-transaction breach notification, among others — remained in the harmonization stage at the Ministry of Law as of October 2025. In the interim,

national compliance oversight is exercised by the Directorate General for Digital Space Supervision under the Ministry of Communication and Digital Affairs (Komdigi), pursuant to Komdigi Ministerial Regulation No. 1/2025. A 2021 study by the then Ministry of Communication and Informatics estimated that Indonesia would need at least 140,917 Data Protection Officers (DPOs) nationwide to satisfy the Law's institutional requirements, while also noting the absence of any official certification scheme for the DPO profession — a capacity gap that persists regardless of whether formal appointments are made. The ambiguity surrounding the Law's qualitative thresholds for mandatory DPO appointment (Article 53) — "large-scale processing" and "systematic monitoring," without numerical criteria — became the subject of a judicial review at the Constitutional Court (Decision No. 151/PUU-XXII/2024, decided 30 July 2025), which affirmed that personal data protection is inseparable from the constitutional right to self-protection under Article 28G(1) of the 1945 Constitution, while leaving the practical threshold question to future implementing regulation.

While the PDP Law's mandate is uniform and centralistic, Indonesia's decentralized governance reality produces asymmetric local capacity: disparities in technological capability, fiscal capacity, and regulatory literacy across regions risk what prior research on regional digital governance terms a fragmentation of protection, in which the security of citizens' data depends on where they happen to live.

1.3 Literature Review and Theoretical Framework

Prior empirical research. Existing empirical work on PDP compliance is dominated by quantitative-

technical assessments — for example, Gao, Sun, and Wang's (2023) decision-tree model for balancing government data openness with privacy in China, and Chatsuwan et al.'s (2023) compliance-assessment case study of government agencies — or by national-scale studies situated outside Indonesia, such as He and Chen's (2025) account of China's PDP trajectory and Nnko et al.'s (2026) assessment of organizational readiness in Tanzania. Jin and Wang (2025) examine smart-city data protection from a multi-stakeholder perspective, while Kamm, Bogdanov, Brito, and Ostrak (2024) propose blueprints for privacy-enhancing technologies in e-government. None of this literature examines how PDP governance is constructed in a locality operating under an asymmetric, constitutionally privileged institutional arrangement — a condition Indonesia shares with only a small number of jurisdictions internationally, yet one that has received little dedicated empirical attention in the personal-data-governance literature.

Institutional theory. Institutional theory frames organizations as subject to coercive, mimetic, and normative pressures that drive structural convergence, independent of technical efficiency (DiMaggio & Powell, 1983). Scott (2008) further distinguishes three institutional pillars: the regulative pillar (formal rules, laws, and sanctions, operating through surveillance and the threat of sanction), the normative pillar (values and norms that bind behavior through social obligation and a sense of appropriateness rather than fear), and the cultural-cognitive pillar (shared, taken-for-granted frames of meaning so deeply embedded that alternatives are not even considered legitimate options). A central construct within this tradition is Meyer and Rowan's (1977) distinction between ceremonial and substantive compliance: organizations frequently adopt formal structures to secure external legitimacy while decoupling those structures from actual operating practice. DiMaggio and Powell (1983) identify three mechanisms that drive such institutional convergence: coercive isomorphism (pressure from regulation or from organizations on which one depends), mimetic isomorphism (imitation of other organizations' practices under conditions of uncertainty), and normative isomorphism (the spread of shared professional standards and vocabularies). This study uses these constructs as its principal analytic lens for

interpreting the relationship between Yogyakarta's formal regulatory instruments and its everyday data-handling practice.

Street-level bureaucracy. Lipsky's (1980) theory of street-level bureaucracy holds that policy is substantively made not by legislators but by the frontline officials who exercise discretion in applying it. Central to this discretion are coping mechanisms such as rationing (limiting service scope or eligibility under resource constraints) and client processing (routinizing how diverse clients are categorized and handled) — mechanisms this study finds directly relevant to how Yogyakarta's apparatus manages a transient population category the PDP Law does not explicitly address.

Collaborative governance. Ansell and Gash's (2008) collaborative governance framework conceptualizes effective multi-stakeholder governance as unfolding through a sequence of conditions: favorable starting conditions (prior relationships, incentives, and power/resource asymmetries among stakeholders), institutional design (clear ground rules, inclusiveness, and process transparency), and facilitative leadership that mediates dialogue and builds trust. Emerson, Nabatchi, and Balogh's (2012) subsequent integrative framework further distributes leadership across sponsor, champion, and facilitator roles rather than concentrating it in a single formal hierarchy. This study uses this staged framework to interpret Yogyakarta's academic-civic ecosystem as an external accountability mechanism and, normatively, to model cross-hierarchy leadership between the Mayor and the DIY Governor without requiring prior resolution of formal authority.

Political economy of bureaucracy. Niskanen's (1971) budget-maximizing model and Wilson's (1989) typology of bureaucratic organizations — procedural, craft, coping, and production organizations, distinguished by the observability of outputs and outcomes — offer a lens for understanding how organizational character and leadership framing shape policy priorities. This study finds that Diskominfo's organizational character shifts across policy domains depending on how leadership frames the issue at stake, a nuance that extends Wilson's typically stable characterization of organizational type.

Integration across levels of analysis. These four frameworks operate at different but complementary levels: institutional theory at the macro (institutional-environment) level, explaining why coercive pressure from the PDP Law dominates without resistance from DIY's special-autonomy legitimacy, and why compliance follows a substance-without-formality pattern; street-level bureaucracy at the micro (individual-apparatus) level, explaining how frontline discretion inadvertently produces outcomes aligned with data minimization; collaborative governance at the meso (inter-organizational) level, explaining why collaborative capital is strong at the starting-conditions stage but has not yet matured into institutional design; and political economy of bureaucracy, also at the meso level, explaining the shifting organizational character of Diskominfo across policy domains as shaped by leadership framing.

1.4 Research Questions and Objectives

This study asks: how is personal data protection governance constructed through institutional structure, street-level administrative capacity, and sociopolitical-leadership dynamics in Yogyakarta City, in the context of the DIY special-autonomy regime, a strong academic ecosystem, and a heterogeneous resident population, following the expiry of the PDP Law's transition period? Three sub-questions guide the inquiry: (1) how are institutional structures and inter-agency coordination mechanisms — including the relationship between Yogyakarta City government and the DIY provincial government in digital and data affairs — constructed and operated; (2) how does municipal apparatus capacity to understand and internalize PDP principles shape governance quality at the operational level, particularly given the demands of a heterogeneous population; and (3) what sociopolitical and leadership factors advance or constrain PDP governance implementation, and how does the DIY special-autonomy context, the academic ecosystem, and the civil-society tradition shape its distinctive character.

1.5 Significance and Scope

Yogyakarta City offers a theoretically productive site for this inquiry. It is embedded within the Special Region of Yogyakarta (DIY), Indonesia's only province governed under its own constitutional statute, Law No.

13/2012, which grants five specific areas of special authority. The city additionally hosts one of Indonesia's densest concentrations of higher-education institutions, produces the nation's highest gross enrollment ratio in higher education, and manages a resident population far smaller than its functional daily population once students, workers, and tourists are included. This combination of asymmetric institutional authority, a historically assertive academic-civic ecosystem, and a demographically heterogeneous data-subject population makes Yogyakarta a critical case for understanding how national PDP mandates are locally constructed under conditions unlike those examined in prior PDP governance research. To strengthen the transferability of a single-case design, the study's findings are triangulated against secondary comparative analysis of five international data-protection regimes and three other Indonesian local governments, including one — Bantul Regency — that shares the same DIY special-autonomy status.

2. Methodology

2.1 Design

This study adopts a qualitative approach grounded in interpretive constructionism, treating PDP governance in Yogyakarta City as a socially constructed reality whose meaning is accessed through the perspectives of actors directly engaged in its practice. The core research strategy is a single case study (Yin, 2018), with Yogyakarta City government as the case and its constituent agencies — the Office of Communication, Informatics and Cryptography (Diskominfo) and the Office of Population and Civil Registration (Dindikcapil) — as embedded units of analysis. To enrich interpretation of this single case without claiming statistical generalization, the primary analysis is supplemented by two forms of secondary comparative analysis: (1) a comparison against the data-protection regulatory frameworks of five jurisdictions (the European Union, Singapore, Malaysia, China, and Thailand), and (2) a comparison against the regulatory patterns of three other Indonesian local governments (Surakarta City, Pekalongan City, and Bantul Regency). Both comparative strands draw on secondary documentary and literature sources rather than primary fieldwork at those sites, and function as interpretive

context for the main case rather than as units of analysis equivalent to Yogyakarta City itself.

The study's analytical framework rests on three integrated layers, aligned with the theoretical framework above. The structural layer draws on Digital Maturity Model concepts (Kane, Palmer, Phillips, Kiron, & Buckley, 2015) to evaluate institutional readiness across governance, human-resource capacity, and technology infrastructure; because the quantitative maturity survey originally envisioned in the research proposal could not be administered, maturity scores reported in this study are qualitative expert judgments by the research team based on triangulated forum and documentary evidence, not the output of a psychometrically validated instrument, and should be read as a communicative device rather than a statistically comparable score. The relational layer draws on the multi-stakeholder governance model (Almeida, Getschko, & Afonso,

2015) to analyze coordination dynamics among government, civil society, the private sector, and academia. The contextual layer comprises the secondary comparative analysis described above.

2.2 Participants/Sample

Primary data derive from one focus group discussion (FGD) conducted on 22 July 2026 at the Diskominfo office. Fourteen external informants participated, as summarized in Table 1: seven Diskominfo officials (the Head of Office and section heads across public information and communication, cryptography and telecommunications, and information systems and statistics), two Dindukcapil staff, two academics, one press/civil-society representative (Indonesian Journalists Association, PWI), one general-public representative, and one private-sector/IT-industry representative

Table 1 Composition of Focus Group Discussion Participants

Stakeholder Group	Role/Position	N
Diskominfo apparatus	Head of Office; heads of Public Information and Communication, Cryptography and Telecommunications, and Information Systems and Statistics Divisions; working-team leads and staff	7
Dindukcapil apparatus	Staff, population administration information management	2
Academia	Representatives of university	2
Press/civil society	Indonesian Journalists Association (PWI)	1
General public	Practitioner	1
Private sector/IT industry	Practitioner	1
Total		14

Compared with the original sampling matrix envisioned in the research proposal (approximately 23 informants across eight categories), three informant categories were not reached in this round of data collection: city executive leadership (the Regional Secretary or the Assistant for Government Affairs),

officials of the DIY provincial Communication and Informatics Office, and university students as a category distinct from the general public.

2.3 Instruments

The FGD was structured around a semi-structured interview guide organized by the study's three analytic dimensions — institutional structure (D1), apparatus capacity (D2), and sociopolitical-leadership dynamics (D3) — with follow-up probes. Secondary instruments comprised documentary analysis of official regulations retrieved through Yogyakarta City's official legal-documentation network (JDIH), an internal digital-competency survey of approximately 5,600 civil servants administered by the city government, and secondary literature and policy documents supporting the international and domestic comparative analyses.

2.4 Procedure

Transparency about method is essential to this study's credibility claims. The original research proposal specified a multi-method, sequential explanatory design: an initial quantitative Digital Maturity Model survey across cities of contrasting digital maturity, followed by approximately 23 individual semi-structured interviews, two separate FGD sessions, non-participant observation, and structured field-documentation review. In execution, field-access and time constraints narrowed the study to a single locus (Yogyakarta City), with primary data collection realized entirely through one combined FGD rather than a validated quantitative survey. The maturity assessment reported in this study therefore reflects the qualitative expert judgment of the research team based on forum and documentary evidence, not a psychometrically validated measurement instrument. This adjustment is reported openly so that readers can accurately calibrate the scope and limits of the findings that follow. Verbal informed consent was obtained from all FGD participants prior to recording.

2.5 Data Analysis

Transcript data were analyzed through thematic analysis (Miles, Huberman, & Saldaña, 2014), organized around dimensions D1–D3 and subsequently elaborated through the four theoretical lenses described in Section 1.3. Secondary documentary and comparative data were triangulated against FGD findings, following Creswell and Poth's (2018) approach to strengthening the credibility of qualitative case-study designs through multiple data sources. Given the single-source primary design, the triangulation actually achieved was within-

forum triangulation (comparing perspectives across government, academic, civil-society, and industry participants present in the same session) and secondary-source triangulation (normative documents and comparative data verified through independent search), rather than the cross-method, cross-institution triangulation the original design intended.

3. Results

3.1 Research Setting

Yogyakarta City is one of five second-tier regions within DIY province, the smallest by area (32.5 km²), administratively divided into 14 kemantren (sub-districts) and 45 kelurahan (urban villages) — the term kemantren is deliberately retained rather than the generic kecamatan used elsewhere in Indonesia, as a marker of DIY's distinct institutional nomenclature. The 2020 national census recorded a population of 373,589; municipal administrative data for 2025 recorded 415,779 — a roughly 11 percent increase, though the two figures derive from different enumeration methods and should be compared cautiously. The city has consistently recorded the highest population density among DIY's regencies and cities. The current Mayor, Hasto Wardoyo, has served since 20 February 2025.

DIY's special status derives from Law No. 13/2012, which designates DIY as the only Indonesian province governed by its own constitutional statute. Article 7(2) of this Law limits DIY's special authority to five domains: (a) the procedure for filling the Governor/Vice-Governor position; (b) DIY's regional institutional arrangement; (c) culture; (d) land tenure; and (e) spatial planning — a closed, textually limitative list rather than an open category subject to administrative expansion. Communication and informatics affairs are not among these five domains. Formally, therefore, data and information-system governance in Yogyakarta City falls under the general regional-autonomy framework of Law No. 23/2014 rather than the special-autonomy regime — although the broader institutional architecture of city agencies, including Dindukcapil's founding regulation, does reference DIY's special regional statute (Special Regional Regulation, or Perdas, No. 3/2015) as part of its legal basis.

Diskominfo was formed in 2016 through the merger of three previously dispersed functions (public relations, information technology/telematics, and cryptography) under Regional Regulation No. 5/2016, with its organizational structure subsequently adjusted several times (Mayoral Regulations No. 79/2016, No. 81/2017, No. 109/2020, and No. 105/2021) in line with national bureaucratic-simplification policy. Its current legal basis is Mayoral Regulation No. 37/2023, comprising the Head of Office, a Secretariat, and four divisions: Public Information and Communication; Information Systems and Statistics; Telematics Infrastructure; and Cryptography and Telecommunications. Its operational mandate for information and communication technology is reinforced by Regional Regulation No. 10/2021 on the Management and Utilization of Information and Communication Technology, elaborated through Mayoral Regulation No. 21/2024, which covers SPBE (electronic-based government system) governance, ICT planning and standardization, data-sharing mechanisms, information-security systems, and SPBE audit and coordination. Dindukcapil, established in 2008 under Regional Regulation No. 10/2008, is currently structured under Mayoral Regulation No. 102/2021, comprising the Head of Office, a Secretariat, and divisions for population registration services, civil registration services, and — most directly relevant here — population administration information management and data utilization.

The population served by Yogyakarta's data systems extends well beyond its registered residents. Alongside 415,779 registered residents, DIY province recorded the nation's highest gross enrollment ratio in higher education in 2024, reinforcing Yogyakarta's identity as Indonesia's "student city" through institutions including Universitas Gadjah Mada, Universitas Negeri Yogyakarta, Universitas Islam Indonesia, and Universitas Ahmad Dahlan; a precise, verified count of Yogyakarta-specific student numbers could not be established in this study, so the widely cited estimate of approximately 300,000 students should be treated as unverified. The city recorded 10,939,210 tourist visits in 2024 (approximately 10.58 million domestic and 355,333 international visitors). As a comparative indicator of digital governance maturity, Yogyakarta's SPBE (electronic-based government system) Index

stood at 3.49 out of 5 in 2024, above the national average of 3.12 and approaching the threshold for the "Very Good" category.

3.2 Status of PDP Implementation

As described in Section 1.2, the national Data Protection Agency mandated under Article 58 of the PDP Law remained unformed at the time of this study, with interim oversight exercised by a Komdigi directorate. At the city level, a search of Yogyakarta's official legal database (JDIH) identified no regulation explicitly implementing the PDP Law's specific obligations — no mayoral regulation on DPO appointment, DPIA procedure, or a breach-notification standard operating procedure under Article 46. Existing derivative regulation is nonetheless substantial: Regional Regulation No. 10/2021 and its implementing Mayoral Regulation No. 21/2024 include an explicit chapter on "data-sharing mechanisms." The instrument closest in substance to PDP implementation is Mayoral Regulation No. 64/2025 on the Information Security Management System (SMKI), enacted 12 December 2025 to replace Mayoral Regulation No. 113/2019. Built on the ISO/IEC 27001:2022 standard and establishing a Government Chief Information Security Officer (GCISO) role and an SMKI Team, this regulation treats personal data protection as a single clause within a broader information-security framework rather than as free-standing PDP implementation. This pattern — an information-security regulation grounded in ISO/IEC 27001, rather than a PDP-specific regulation — traces to national mandates under Ministry of Administrative and Bureaucratic Reform (PANRB) Regulation No. 5/2020 and National Cyber and Crypto Agency (BSSN) Regulation No. 4/2021, and is not unique to Yogyakarta, as the domestic comparison in Section 3.8 confirms.

3.3 Institutional Structure and Coordination

Centralized technical authority, diffused compliance responsibility. The Head of Diskominfo confirmed that only Diskominfo is authorized to build digital service applications for Yogyakarta City government; Dindukcapil, the Health Office, and the Education Office are not permitted to develop their own applications, with all development centralized under Diskominfo's supervision through

its Information Systems and Statistics, Telematics Infrastructure, and Cryptography divisions. Operational security control runs through the Cryptography Communication Network (Jaring Komunikasi Sandi, JKS) Team, whose members are stationed across city agencies. No evidence of a formally designated PDP Officer (DPO) was identified, consistent with the absence of PDP-specific regulation noted in Section 3.2. Asked directly about a dedicated PDP division, the Head of Diskominfo stated that responsibility for data protection "remains attached to whichever agency directly manages and controls the data in question." Accountability instead operates through inter-agency service-level agreements (SLAs) and non-disclosure agreements (NDAs), supplemented by data redaction practices under the Public Information Management Officer (PPID) framework for public-information services.

An operative incident. The JKS Team's routine monitoring detected the use of unlicensed operating-system software in one city agency — a vulnerability directly relevant to the PDP Law's data-security obligations (Articles 35–39), since unlicensed software typically lacks vendor security patches. This case offers concrete evidence that Yogyakarta's informal oversight mechanism functions in practice rather than existing only as rhetorical claim. However, the available transcript does not specify which agency was involved, the interval between detection and remediation, whether the incident met the threshold for mandatory breach notification under Article 46, or whether it was formally documented for future audit — a gap that illustrates a recurring pattern in this study's findings: strong technical detection capacity within the existing information-security framework, but weak procedural-administrative follow-through on the specific requirements the PDP Law newly introduces.

Cross-agency and vertical coordination. Contrary to an initial expectation of restricted data access, the Head of Diskominfo described a pattern of excessive openness: a request for aggregate data was sometimes answered by data-providing agencies with more complete information than requested, including individual names and addresses — an issue the informant attributed to data handlers' limited literacy regarding PDP boundaries rather than to the access

architecture itself. Vertical coordination with the DIY provincial government follows a "one-data" principle: aggregate data flows upward to the provincial and national levels, while personal-level data remains managed at the city level, through a coordinative rather than a hierarchical-responsibility relationship.

Testing the special-autonomy hypothesis. The most theoretically significant finding concerns the special-autonomy question directly. Asked explicitly about PDP coordination structures with the DIY provincial government, the Head of Diskominfo stated unambiguously that DIY's special authority applies only to cultural and administrative-nomenclature matters (for instance, the terms *kemantren* for sub-district and *kudha* for provincial agencies), not to data-governance structure, articulating the operating principle that "whoever manages and controls the data is who is responsible, not a matter of structural hierarchy to the province." This empirical finding is consistent with the normative analysis in Section 3.1 — that communication and informatics affairs fall outside DIY's five special-authority domains — yet it directly tests, rather than merely confirms, the authority-ambiguity hypothesis this study's conceptual framework proposed. Two readings of this finding warrant consideration: (1) the PDP Law's coercive national mandate operates without meaningful resistance from DIY's special-autonomy legitimacy in the data domain; or (2) a single official's response, from the City government's own institutional representative, may partly reflect ceremonial institutional self-presentation, which would require cross-verification with DIY provincial informants — unavailable in this dataset — to resolve.

A risk beyond municipal control. Informants also described cases of third parties impersonating Dindukcapil, Taspen, or BPJS (the national social-security agency) around the rollout of digital ID cards, exploiting public trust in these institutions to solicit additional personal data or direct citizens to fraudulent links — a social-engineering pattern common to national digital-policy rollouts elsewhere, not a vulnerability specific to Yogyakarta. This case illustrates that not all data-protection risk to Yogyakarta's residents can be mitigated through improvements to city-level governance alone; some risks require

mitigation at the national level, through public digital-literacy campaigns explaining how legitimate institutions communicate.

3.4 Apparatus Capacity

The Head of Diskominfo explicitly contrasted Yogyakarta's challenge with prior comparative research in Depok City, characterizing Depok's central challenge as general digital-literacy deficits, while framing Yogyakarta's challenge as one of behavioral internalization — citing, for example, the common local practice of citizens lending their identity cards to others for document processing, and instances of publicly accessible voter data at polling stations.

On managing the heterogeneous population, the city's approximately 415,000 registered residents sit against an informant-estimated daily functional population of 1.3 to 1.5 million. Apparatus competence here is expressed through three operational policies: a principle of not compelling migrants to transfer local residency registration (with emergency services provided irrespective of registration status); passive-informative tracking of non-permanent residents (with formal non-permanent residency applications estimated at only 1–2 percent of the relevant population, largely via boarding-house registration); and restriction of tourism data collection to the aggregate level. Read through street-level bureaucracy theory, these practices function as rationing and routinization that functionally approximate the PDP Law's data-minimization principle, even without explicit reference to the Law as their basis.

An internal digital-competency survey of approximately 5,600 civil servants found personal-data-security awareness to be the relatively weakest dimension measured among digital competencies assessed — a finding that aligns closely with the national pattern: Indonesia's Digital Literacy Index has consistently shown digital security as its weakest pillar year over year. Notably, DIY recorded the nation's highest Digital Literacy Index score among Indonesia's 34 provinces in 2021 (3.71), well above the national average (3.49) — an analytically valuable paradox indicating that the digital-security gap is a structural, nationally systemic pattern rather than a function of a region's general digital-literacy level. Training occurs

through the monthly Jaring Komunikasi Sandi (JKS) forum, using competency-survey results to shape curriculum content. Institutional-continuity risk is managed through roughly four-year contract cycles for key personnel, mandatory confidentiality undertakings, and required knowledge transfer prior to staff reassignment.

3.5 Sociopolitical and Leadership Dynamics

Leadership framing. Leadership commitment to PDP was articulated predominantly through a digital-sovereignty narrative rather than direct technical compliance with the PDP Law: the Mayor is described as frequently emphasizing that citizens' transaction data is effectively controlled by unicorn-scale digital platforms (Gojek, Grab, Shopee, Tokopedia) rather than by local businesses or government. Independent verification confirmed that Diskominfo is explicitly positioned as the city's "data custodian" (wali data) within the SPBE framework, consistent with the spirit of the One Data Indonesia policy — an independently confirmed finding that supports the feasibility of Component 5 of the governance model proposed in Section 4.4.

The special-autonomy leadership question. The available data contains no direct informant commentary on the political relationship between the Mayor and the DIY Governor in relation to PDP specifically. This gap is marked explicitly as a limitation requiring dedicated follow-up data collection.

Academic-civic ecosystem as external accountability. An informant from Universitas Islam Indonesia argued, drawing on ICT-for-Development and World Summit on the Information Society (WSIS) framing, that effective digital governance cannot be sectoral but must be ecosystem-based from the policy-formulation stage, not merely incorporate outside actors after a policy is finalized — citing the historical precedent of the Indonesia Internet Exchange (IIX) Jogja, an inter-university infrastructure initiative that subsequently expanded to involve local government, as a working precedent for the Jogja Smart Service (JSS) platform's current service quality. This directly substantiates the study's premise that Yogyakarta's academic-civic ecosystem functions as a genuine,

historically demonstrated collaborative-governance mechanism, not merely a theoretical possibility.

A dissenting citizen voice. This accountability pressure was not uniformly affirmative. The general-public representative, informant, raised concern that residents are frequently "compelled by necessity" to surrender personal data — including biometric data collected by third parties, such as employment social-security (BPJS Ketenagakerjaan) registration — for services unrelated to the data's original purpose, questioning who bears responsibility for protecting citizen data across such inter-institutional boundaries. This concern touches directly on Article 20 of the PDP Law regarding the lawful basis for processing, in tension with the critique that "consent" is not truly free within mandatory service schemes. Two additional sensitive issues — concern about potential misuse of data for political/electoral purposes, and a question about neighborhood CCTV programs ahead of elections — surfaced only through this single informant and are treated as too thin an evidentiary base for substantive conclusions, though their emergence from the forum's only "purely" citizen voice is worth noting as an indication that citizen perspectives may be more critical of digital-surveillance issues than either apparatus or academic perspectives.

Industry perspective. The IT-industry representative, appearing alongside the university academic in a segment on JSS's security-convenience trade-off, offered a technical assessment that JSS "does not require the layered security typical of banking applications" — a position notably aligned with government's own risk assessment rather than an independent critical stance, diverging from collaborative-governance literature's common assumption that private-sector participants bring systematically different interests from government. This alignment is recorded as an open question for future research rather than a settled interpretation, since the available data cannot determine whether it reflects genuinely independent technical judgment or an unexplored business relationship with the city government.

A gradient of critical distance. Reading the FGD data by informant group reveals a pattern not fully visible in the thematic analysis merged across groups:

the apparatus (closest to government) expressed the most affirmative tone; academics (an intermediate distance, with institutional interest in long-term collaboration) expressed a mixed tone — analytically supportive from university, technically neutral from university; while the citizen representative (furthest from formal government structure) expressed the most critical tone. Notably, the press/civil-society representative — theoretically expected to occupy a critical position comparable to the citizen representative, given its watchdog function — left no analyzable data trace in this forum, a gap recorded as a limitation.

Framing analysis across informant groups. A closer reading of how, not merely what, each informant group communicated about PDP governance reveals that the four groups were substantively answering different underlying questions when asked about ostensibly the same issue: the apparatus framed PDP as a matter of digital-economic sovereignty (data ownership vis-à-vis external platforms, echoing the political economy of bureaucracy); practioner academic informant framed it as ecosystem-based governance design (inclusiveness from the policy-formulation outset, echoing collaborative governance); university and the industry representative framed it as a technical security-convenience trade-off (proportionality of security to data sensitivity, a risk-based compliance framing); and the citizen representative framed it as a matter of fairness and individual accountability (who is responsible when data is misused, echoing meaningful consent). This divergence is not merely rhetorical variation but reflects a fundamental difference in what each group considers the core issue. A multi-stakeholder forum designed without accounting for this framing diversity risks a dialogue in which participants discuss the same topic while substantively addressing different concerns — a classic risk in multi-sector collaborative governance.

Impact on vulnerable groups. Three vulnerable groups deserve explicit attention, given their structural exposure to governance risk yet minimal representation in this study's data. The security-convenience trade-off discussion explicitly implicated elderly residents, with UNIVERSITY and industry informants noting that additional verification layers risk impeding this group's

access to digital services — a genuine tension between stricter data-security compliance (Articles 35–39) and inclusive access, on which this study contains no direct elderly-resident perspective. Students, despite constituting the largest component of Yogyakarta's non-permanent population and a central justification for this study's site selection, were not represented as a distinct informant category; policies concerning student data are therefore formulated and evaluated solely from the service-provider perspective. Citizens with limited digital literacy are similarly least equipped to negotiate the terms of digital services they use, a vulnerability implicit in informant concern about being "compelled by necessity" to surrender personal data. These gaps underscore a methodological limitation: research relying on a single forum dominated by service providers

structurally tends to under-capture the perspective of service recipients, particularly the most vulnerable.

3.6 Compliance Crosswalk

To translate the preceding narrative findings into a form immediately usable by practitioners, Table 2 maps the PDP Law's substantive chapters against verified evidence of Yogyakarta's compliance status. Status labels ("Present," "Partial," "Not Found") reflect evidence verified within this study's data (FGD transcript and public document search), not a definitive claim that a given mechanism is entirely absent; several "Not Found" entries could shift to "Present" if future research gains access to internal documents beyond this study's reach.

Table 2 Compliance Mapping: PDP Law Articles Against Yogyakarta City's Documented Status

PDP Law Provision	Core Requirement	Status	Evidence
Arts. 5–13 (data-subject rights)	Access, correction, erasure, consent withdrawal, objection, portability	Not found	No formal request channel beyond the general PPID public-information channel
Arts. 20–24 (lawful basis & consent)	Processing must rest on consent or another lawful basis	Partial	JSS privacy policy requires consent; data-restriction practice reflects due care, but legal basis not consistently cited
Arts. 30, 32, 40–41 (procedural deadlines)	Data update/access and processing-suspension requests fulfilled within 3×24 hours	Not found	No SOP identified as a recognized apparatus procedure
Art. 34 (DPIA)	Mandatory impact assessment for high-risk processing	Not found	Not mentioned as an operating practice
Arts. 35–39 (data security)	Protect security, confidentiality, and oversee involved parties	Partial, via SMKI	Mayoral Reg. No. 64/2025 (SMKI), JKS Team, SLA/NDA mechanisms
Art. 46 (breach notification, 3×24 hours)	Mandatory written notification to data subjects and the supervisory authority	Not found	A real incident (unlicensed software) was detected, but notification follow-through unconfirmed

Arts. 53–54 (DPO appointment)	Mandatory appointment for government agencies and large-scale processing	Not found	Confirmed by the Head of Diskominfo: responsibility diffused to agencies, no formal DPO
Arts. 62–64 (public participation)	Government must facilitate information and encourage active participation	Not found	No dedicated PDP participation/education channel, distinct from general PPID requests

The pattern emerging from this crosswalk reinforces the study's central conclusion: compliance concentrates on obligations intersecting the pre-existing information-security domain (Arts. 35–39, partly met through SMKI) and on informal data-restriction practice, while obligations with strict procedural deadlines and specific personnel designation (Arts. 46, 53–54) show no identified evidence. The near-total absence of a public-participation mechanism (Arts. 62–64) is consistent with the absence of a recorded press/civil-society voice in this study's data.

3.7 International Comparative Analysis

To assess Yogyakarta's position proportionately, this section benchmarks Indonesia's PDP Law against five widely referenced data-protection regimes: the European Union's General Data Protection Regulation (GDPR), Singapore's Personal Data Protection Act (PDPA), Malaysia's PDPA, China's Personal Information Protection Law (PIPL), and Thailand's PDPA (Table 3).

GDPR's Article 37(1)(a) requires DPO appointment unconditionally for any public authority, a stricter

standard than for private organizations. Singapore's and Malaysia's PDPAs, both enacted over a decade before Indonesia's, only introduced mandatory breach notification and DPO appointment through 2024–2025 amendments — thirteen and fourteen years after their original laws, respectively — and Singapore historically excluded public agencies from direct coverage altogether. China's PIPL offers a contrasting quantitative approach: DPO appointment is triggered by numerical thresholds (over 200 employees, or processing data of over 1,000,000 individuals, or sensitive data of over 100,000) rather than the qualitative-categorical language shared by GDPR and Indonesia's PDP Law. Thailand's PDPA, whose enforcement was itself delayed twice before taking full effect in 2022, sets DPO criteria structurally near-identical to Indonesia's Article 53(1); tellingly, Thailand's own qualitative criteria for "large scale" and "systematic monitoring" only received official clarification four years after enactment — evidence that this ambiguity is a common design challenge of principle-based regulation generally, not a defect unique to the PDP Law.

Table 3 Comparative Data-Protection Regulatory Frameworks

Aspect	GDPR (EU)	Singapore PDPA	Malaysia PDPA	China PIPL	Thailand PDPA	Indonesia PDP Law
DPO obligation	Mandatory, unconditional for public bodies	Mandatory from 2025 (13 yrs. after enactment)	Mandatory from 2024 (14 yrs. after enactment)	Mandatory; quantitative thresholds	Mandatory; criteria clarified 2023 (4 yrs. after)	Mandatory from enactment; qualitative criteria (Art. 53)

Breach notification	Max. 72 hours	Mandatory from 2025	Mandatory from 2024	Mandatory from enactment	Mandatory upon full enforcement (2022)	Max. 3×24 hours (Art. 46)
Public-sector coverage	Explicit; DPO required	Historically excluded	Varies by sector	Covers public & private	One of three mandatory-DPO categories	Explicit; all levels of government
Supervisory authority	DPA per member state (2018)	PDPC (2013)	JDPD (2013)	Cyberspace Admin. of China	PDPC Thailand	Not yet formed; interim Komdigi oversight
Maximum penalty	4% global turnover or €20M	Up to 10% turnover	RM 1M (≈ IDR 3.9B)	Up to RMB 50M or 5% turnover	Prison ≤1 yr. and/or ≤5M Baht	≤2% annual revenue (Art. 57); criminal ≤IDR 6B

This comparison yields four observations. First, Indonesia is not behind on legal design: the PDP Law adopted DPO and breach-notification obligations from the outset — elements Singapore and Malaysia only added through 2024–2025 amendments, years after their original laws took effect. Second, Indonesia's gap lies in enforcement infrastructure, not normative design: GDPR, Singapore, and Malaysia have all had operating independent supervisory authorities since their laws' early years, while Indonesia relies on interim Komdigi oversight pending the Data Protection Agency's formation. Third, Indonesia's textual coverage of the public sector is more explicit than Singapore's, whose PDPA historically excluded public bodies altogether — meaning Yogyakarta's legal obligation to appoint a DPO rests on grounds no less firm than in many advanced economies; the outstanding issue is execution, not ambiguity. Fourth, Indonesia's qualitative-categorical approach carries an inherent weakness relative to China's quantitative approach: "large-scale processing" and "systematic monitoring" thresholds under Article 53 remain open to interpretation — the very ambiguity that reached the Constitutional Court (Decision No. 151/PUU-XXII/2024) — while Thailand's experience shows that

even comparable qualitative jurisdictions require years to achieve regulatory clarity.

This international benchmarking reinforces, rather than undermines, the argument that Yogyakarta City has sufficient legal basis to formalize a DPO structure immediately, without waiting for national implementing regulation. As a public body processing citizens' personal data, Yogyakarta clearly falls within the mandatory-DPO category under Article 53(1)(a) — a classification that does not depend on the issuance of an implementing government regulation or the Data Protection Agency's formation. Singapore's and Malaysia's more-than-decade-long delay in "catching up" to standards Indonesia possessed from the outset is a cautionary reminder that waiting for full central-authority certainty is not necessarily the wiser strategy.

3.8 Domestic Comparative Analysis

Narrowing the comparative lens to a more practically relevant scale, this section examines how three other Indonesian local governments — including one within DIY itself — have responded to information-security and data-protection obligations.

Surakarta City's Mayoral Regulation No. 29/2025 on the Electronic-Based Government Information

Security Management System establishes an institutional structure resembling Yogyakarta's pattern, with an SMKI Team appointed by the mayor, referencing the ISO/IEC 27001 standard. Pekalongan City shows more advanced progress on one dimension: through Mayoral Regulation No. 74/2023 on SPBE Information Security Management, its communication and informatics office did not stop at issuing regulation but obtained independent ISO/IEC 27001:2022 certification for its application-services and IT-infrastructure scope — third-party verification that is methodologically stronger evidence of compliance than regulation alone, since regulation demonstrates intent while certification demonstrates externally verified implementation. This study found no evidence that Yogyakarta has pursued comparable certification; its Mayoral Regulation No. 64/2025 references ISO/IEC 27001:2022 only as a framework standard, not as an independently certified standard.

The most methodologically relevant finding is Bantul Regency's Regent Regulation No. 35/2023 on the Information Security Management System — a regency directly bordering Yogyakarta City, sharing the same DIY province and special-autonomy framework. This regulation establishes an Information Security Committee (Komite Keamanan Informasi, KKI), a cross-agency collective decision-making body, with technical teams in each agency. This finding matters for two reasons. First, it shows the SMKI-based (rather than PDP-specific) pattern found in Yogyakarta is replicated within DIY province itself, reinforcing that DIY's special autonomy does not produce a systematically distinct data-governance approach even among localities in the same province. Second, Bantul's KKI — with genuine decision-making authority, unlike a mere technical monitoring team — offers an alternative institutional model for Yogyakarta, potentially a more suitable vehicle for integrating DPO functions than attaching sole responsibility to a single division, as proposed under Component 1 of the Adaptive PDP Governance Model (Section 4.4).

This replication pattern across Surakarta, Pekalongan, Bantul, and Yogyakarta traces to national

regulations that indirectly encourage uniformity: beyond PANRB Regulation No. 5/2020 and BSSN Regulation No. 4/2021, Ministry of Home Affairs Regulation No. 17/2023, Article 18A(1), requires every user of population data to apply security standards prioritizing ISO 27001 as a condition for data utilization. This explains why the SMKI/ISO 27001 framework has become a far more consistent reference across local governments than the PDP Law's more specific technical requirements: the Ministry of Home Affairs has issued a clear SMKI/ISO 27001 mandate, while an equivalent technical mandate for the PDP Law has not yet been issued by any ministry or agency.

Yogyakarta's comparative position can therefore be summarized as follows: at the general information-security (SMKI) level, Yogyakarta is on par with Surakarta and Bantul, though one step behind Pekalongan, which has achieved independent certification. At the PDP-specific regulatory level (DPO, DPIA, breach notification), none of the compared cities/regencies — including Yogyakarta — show meaningful progress, confirming that this gap is systemic-national rather than a failure specific to Yogyakarta. Notably, no city or regency identified in this comparison has yet claimed the position of a PDP-specific regulatory pioneer at the local level — a position Yogyakarta's existing leadership momentum and tested institutional capital place it in a comparatively favorable position to claim first.

3.9 Governance Maturity Assessment

To complement the narrative and article-by-article findings, this study proposes a maturity matrix converting qualitative findings into standardized scores per indicator, following a common four-level maturity scale (1 = Initial/Ad hoc, 2 = Developing, 3 = Mature, 4 = Optimal). As emphasized in Section 2.1, these scores are qualitative expert judgments by the research team based on FGD and documentary evidence, not the output of a psychometrically validated instrument, and should be read as a communication aid rather than a definitive score for statistical comparison with other regions absent an equivalent assessment methodology.

Table 4 Governance Maturity Matrix for Yogyakarta City's PDP Governance, by Indicator

Dimension	Indicator	Score	Justification
-----------	-----------	-------	---------------

D1 — Institutional	Formal DPO	1	No formal appointment; diffused to agencies
D1	PDP-specific regulation	1–2	Exists (ICT/SMKI Reg.) but no PDP terminology
D1	Informal accountability (SLA/NDA/JKS)	3	Proven functional; detected a real incident
D1	Breach-notification SOP	1	No formal SOP identified
D2 — Capacity	Data minimization competence	3	Mature, consistent heterogeneous-population policy
D2	Individual data-security awareness	2	Weakest dimension; active improvement program
D2	Dedicated PDP budget	1	No line item separate from general digital budget
D2	Ongoing training (JKS forum)	3	Regular monthly cadence, survey-based curriculum
D3 — Sociopolitical	Leadership commitment	3	Digital-sovereignty framing, independently corroborated
D3	Collaborative capital	3	IIX Jogja precedent; active academic-civic ecosystem
D3	Formal DIY coordination	1–2	One-data principle exists; no explicit PDP coverage
D3	Public participation	2	Critical citizen voice exists but not institutionalized

The weighted average across all twelve indicators is 2.08 of 4 ("Developing"), obscuring a more informative dimension-level pattern. D1 records the lowest average (1.63): a bimodal split between mature informal mechanisms (score 3) and absent formal elements (score 1) — the PDP Law's genuinely new requirements. D3 records the highest average (2.38), driven by leadership commitment and collaborative capital; D2 falls in between (2.25), held back mainly by the absent budget line.

This bimodal D1 pattern indicates the problem is not "generally weak institutions" but selective weakness

on elements the PDP Law newly introduced, implying a "targeted patching" strategy is more efficient than a comprehensive overhaul. D3's two low-scoring indicators (DIY coordination, public participation) also derive partly from an absence of data rather than confirmed poor performance — a nuance distinct from D1's scores, which rest on explicit evidence that a DPO does not exist.

3.10 SWOT Synthesis

As a bridge to the integrated discussion that follows, Table 5 synthesizes internal and external factors bearing

on Yogyakarta's PDP governance strategy, complementing the maturity matrix's internal-condition focus with explicit consideration of external opportunities and threats beyond the City government's direct control.

Table 5 SWOT Analysis of Yogyakarta City's PDP Governance

Category	Factor
Strengths (internal)	SPBE Index above national average (3.49 vs. 3.12); proven informal accountability mechanisms (SLA/NDA, JKS, PPID), including real-incident detection; tested multi-stakeholder collaborative capital (IIX Jogja precedent); mature technical competence in heterogeneous-population data minimization; explicit, independently corroborated leadership commitment ("data custodian" policy)
Weaknesses (internal)	No formal DPO or 3×24-hour breach-notification SOP; derivative regulation has not adopted the PDP Law's technical terminology; no dedicated PDP budget line separate from general digital activity; absence of press/civil-society and student voices in this study's evidentiary base
Opportunities (external)	No comparator city/regency yet identified as a PDP-specific regulatory pioneer; Indonesia's legal basis for public-body DPO obligation is textually equivalent to GDPR and Thailand's PDPA and does not depend on implementing regulation; the existing DIY-level One Data Indonesia forum can be expanded in scope
Threats (external)	Nine implementing government regulations and the national Data Protection Agency remain unformed, with no fixed timeline; absence of direct data from DIY provincial government creates uncertainty about coordination willingness; external risks beyond City control (institutional-identity misuse, centralized national population-data vulnerability)

Cross-reading internal and external factors yields four strategic implications. An SO strategy leverages mature institutional capital and potential first-mover status to formalize the DPO and notification SOP while this opportunity window remains open. A WO strategy addresses the absent PDP budget by integrating it into the already-supported SPBE/One Data budget rather than proposing a free-standing line item. An ST strategy treats the national institutional vacuum as no reason for inaction, since Yogyakarta's collaborative capital and leadership strength suffice to proceed independently on aspects not dependent on the national supervisory authority. A WT strategy mitigates the combined risk of institutional gaps and DIY-coordination uncertainty by initiating informal consultation with the provincial communication and informatics office early, before

Components 1–4 are fully complete, avoiding a compounded scenario in which the city is simultaneously unprepared internally and disconnected from provincial coordination.

4. Discussion

4.1 Substance Without Formality: Revisiting Institutional Theory

The central finding of this study — that Yogyakarta's PDP governance operates through informal, substantively functional mechanisms in the near-complete absence of the formal structures the PDP Law mandates — departs from institutional-compliance literature's dominant expectation that organizations facing coercive regulatory pressure adopt ceremonial formal structures for external legitimacy while decoupling them from operating

practice (Meyer & Rowan, 1977), and from technical-compliance studies elsewhere that treat formal-structure adoption as the primary compliance indicator (Chatsuwan et al., 2023; Gao et al., 2023). This pattern holds consistently across all four theoretical frameworks introduced in Section 1.3, not merely as an artifact of one analytic lens: at the macro level (institutional theory), national coercive pressure operates without structural resistance, yet formal structure remains empty; at the meso level (collaborative governance and political economy of bureaucracy), collaborative capital and leadership commitment are strong, yet institutionalization is incomplete; and at the micro level (street-level bureaucracy), individual discretion produces substantive outcomes without formal regulatory reference. This cross-level consistency strengthens confidence that the pattern is a genuine characteristic of the Yogyakarta case, not a methodological artifact confined to a single level of analysis.

A plausible explanation is that Yogyakarta's data-handling norms predate the PDP Law itself, rooted in the City's pre-existing service-delivery culture, such that substantive practice did not require formal codification to emerge — while the formal instruments the Law specifically requires (a designated officer, an explicit implementing regulation, a dedicated budget line) simply have not yet been produced, plausibly because of the national institutional vacuum documented in Section 1.2 and Section 3.2. Elaborating DiMaggio and Powell's (1983) three isomorphisms sharpens this explanation: mimetic isomorphism (the informal adoption of private-sector-style contractual instruments, namely SLA/NDA) and normative isomorphism (the shared ISO 27001 vocabulary replicated identically across Surakarta, Pekalongan, and Bantul, per Section 3.8) prove as powerful as coercive isomorphism from the PDP Law itself in shaping Yogyakarta's response. This suggests institutional-compliance theory may need to accommodate contexts where regulatory coercion is real, but where local implementation capacity and pre-existing local practice culture — rather than external legitimacy-seeking — are the dominant drivers of observed compliance patterns. This reading nonetheless rests on a single institutional informant (the Head of Diskominfo) and requires

cross-verification before being treated as more than a tentative theoretical proposition, particularly given that the reflexivity analysis in Section 4.6 identifies this same informant as the source of the study's most significant — and least externally verified — claims.

4.2 Street-Level Bureaucracy: Discretion as Anticipatory Compliance

This study's second contribution nuances Lipsky's (1980) classical formulation of discretion as primarily a risk to policy consistency. Evidence in Section 3.4 shows frontline apparatus using rationing (restricting formal registration requirements for non-permanent residents) and client processing (routinized, differentiated handling of resident, student, and tourist data categories) to manage a population category the PDP Law does not explicitly address — and, in doing so, inadvertently producing outcomes functionally aligned with the Law's data-minimization principle, without the apparatus explicitly invoking that principle as their basis. This finding extends the conventional understanding that discretion is chiefly a threat to consistent policy implementation, showing instead that discretion can function as an adaptive mechanism anticipating formal regulation not yet adopted — a nuance rarely emphasized in classical street-level bureaucracy literature, and one made possible in this case by informal practice culture developed well before the PDP Law's enactment.

4.3 Collaborative Governance and the Political Economy of Bureaucracy

Mapping the IIX Jogja precedent onto Ansell and Gash's (2008) staged collaborative-governance process suggests that collaborative capital can be inherited across policy generations (a form of path dependency): favorable starting conditions from a past digital-infrastructure collaboration become capital for newer PDP-specific collaboration. Yet strong starting conditions alone do not automatically yield mature collaborative governance without explicit investment in institutional design and facilitative leadership — precisely the gap identified in Sections 3.5 and 3.9 (Component D3's high average score masking two data-poor indicators). This nuances Ansell and Gash's (2008) framework, which emphasizes trust-building as a general

precondition for effective multi-stakeholder governance without extensively theorizing how that trust might vary by institutional target within the same governance system; this study's evidence of differentiated public trust — high confidence in municipal government specifically, greater caution toward the wider digital ecosystem citizens must navigate for essential services — suggests PDP governance models for similarly civically active localities should treat public trust as a resource specific to the institutions that earned it, not something that extends automatically to the broader digital ecosystem.

Read through the political economy of bureaucracy, the observation that Diskominfo's organizational character shifts across policy domains, depending on how leadership frames the issue, adds nuance to Wilson's (1989) typology, which tends to treat organizational character as a relatively stable attribute. This study suggests organizational character

can instead be fluid and dependent on leadership context — evident in the contrast between the digital-sovereignty framing applied to platform-economy issues (Section 3.5) and the more procedural, compliance-oriented framing applied to routine information-security matters (Section 3.3).

4.4 The Adaptive PDP Governance Model

Synthesizing the empirical findings with the comparative and maturity analyses in Sections 3.6–3.10, this study proposes a six-component Adaptive PDP Governance Model. Components 1–4 are grounded directly in empirical findings; Components 5–6 are literature-based prescriptive recommendations, explicitly marked as such given the absence of direct DIY-provincial or Mayor–Governor relational data. Table 6 summarizes each component's empirical basis, principal implementation step, and main implementation risk; the paragraphs that follow provide brief elaboration only where the table requires interpretive context

. Table 6 Adaptive PDP Governance Model: Components, Basis, and Implementation

Component	Basis	Key Implementation Step	Main Risk / Mitigation
1. Formal DPO designation	Empirical (§3.3, §3.9)	Mayoral Decree appointing a DPO from the existing Cryptography Division; job description referencing Art. 54; breach-notification SOP integrated with JKS incident detection	Administrative delay, not refusal; mitigate by linking urgency to Art. 57 sanctions and Decision No. 151/PUU-XXII/2024
2. Individual capacity and budget	Empirical (§3.4, §3.9)	Dedicated PDP budget line separate from general digital activity; PDP literacy module added to the monthly JKS forum, aligned with the National Digital Literacy Program	Budget constraint; mitigate by starting with the low-cost JKS curriculum revision
3. Codifying heterogeneous-population practice	Empirical (§3.4)	Dindukapil and the Tourism Office jointly issue written guidance codifying existing informal data-minimization practice,	Over-formalization eroding useful discretion; mitigate by framing guidance as principles, not rigid rules

		citing the PDP Law explicitly	
4. Multi-stakeholder forum	Empirical (§3.5, §3.9)	Diskominfo's institutionalizes a routine PDP consultation forum building on the IIX Jogja precedent, deliberately including press/civil-society representation absent from this study	Forum becomes ceremonial; mitigate by mandating periodic review of Components 1–3
5. Formal Pemkot–DIY coordination (prescriptive)	Literature-based	Expand the DIY-level One Data Indonesia forum's agenda to include PDP compliance; the Component-1 DPO serves as standing representative	Feasibility unconfirmed absent DIY-provincial data; requires prior consultation
6. Cross-hierarchy leadership (prescriptive)	Literature-based	Mayor as policy champion, DIY Governor as symbolic-political sponsor, One Data forum secretariat as facilitator (Emerson et al., 2012)	Most speculative component; success depends on political factors beyond this study's reach

Component 1 responds to the single lowest-scoring pair of indicators in Table 4 (formal DPO and breach-notification SOP), and is deliberately designed to formalize existing capacity — the JKS Team's demonstrated incident-detection ability — rather than create an entirely new unit. Component 5 is grounded in Diskominfo's independently confirmed "data custodian" policy (Section 3.5), which supports its feasibility even though direct provincial-level data is unavailable. Component 6 is explicitly the most speculative of the six, since it responds to a complete data gap regarding Mayor–Governor political dynamics; a role-functional approach is deliberately chosen because it does not require detailed understanding of real power dynamics between the two leaders.

Prioritization and roadmap. Cross-referencing these six components against the maturity matrix, the most efficient sequence addresses Components 1 and 2 first, followed by Component 3 (low cost, merely

codifying already-mature practice), then Component 4, and finally Components 5 and 6, which require longer cross-institutional preparation. An indicative quarterly roadmap — to be adjusted against Yogyakarta's actual regional planning-budgeting cycle (RKPD/APBD) — proceeds as follows: Q1 begins Components 1 and 3, producing a draft DPO appointment decree and draft heterogeneous-population guidance; Q2 continues Component 1 while beginning Component 2 and initiating consultation under Component 5, yielding an issued DPO decree, a submitted PDP budget proposal, and a consultation letter to the DIY provincial government; Q3 completes Component 3, continues Component 2, and begins Component 4, integrating PDP training into the JKS forum, issuing the heterogeneous-population guidance, and initiating the multi-stakeholder forum; and Q4 completes the breach-notification SOP under Component 1, continues Component 4, and reviews Component 5's consultation outcome, bringing the notification SOP

into effect and convening the first multi-stakeholder forum. Component 6 is not scheduled as a discrete phase, given its nature as an ongoing relational orientation rather than an administrative output with a fixed completion date.

4.5 Positioning Yogyakarta Nationally and Internationally

Read together, Sections 3.7 and 3.8 establish that Yogyakarta's implementation gap is not a unique local failure. At the international level, comparable — and in some respects slower — gaps were experienced by Singapore and Malaysia, both with substantially more mature institutional capacity. At the domestic level, the SMKI-without-PDP-specificity pattern is replicated precisely in Surakarta, Pekalongan, and within DIY province itself (Bantul Regency), confirming this gap is systemic-national rather than a locally specific deficit. That SMKI-based regulation spread rapidly and uniformly across four studied localities without explicit coordination, while PDP-specific regulation is found almost nowhere among them, suggests local governments are generally prepared to follow standardized technical guidance, provided it is made available — the abundance of SMKI/ISO 27001 guidance juxtaposed with the absence of equivalent PDP-specific guidance appears to be the principal explanatory factor, not local resistance. This positions the Ministry of Home Affairs, as the ministry most directly supervising local governments nationwide, to consolidate good practices already emerging organically — including Bantul's Information Security Committee model — into a nationally replicable template, rather than leaving each region to rediscover its own solution through costly trial and error.

4.6 Limitations

Following standard qualitative validity criteria (credibility, dependability, confirmability, and transferability), several limitations qualify this study's conclusions. On **credibility**, the principal threat is reliance on a single primary data source — one FGD, without the individual interviews and non-participant observation the original proposal envisioned — combined with the dominance of a single institutional voice (the Head of Diskominfo) across many of

the study's most significant findings, including the finding that DIY's special autonomy does not affect data governance. Reflexivity has been applied consistently to anticipate this risk, but reflexivity reduces bias rather than eliminating it entirely. On **dependability**, the realized single combined FGD (rather than the two separate sessions originally planned, with government and non-government participants meeting separately) may have introduced an anchoring effect on non-government participants who answered after hearing the government group's responses first — an effect this dataset cannot measure. On **confirmability**, most substantive claims are explicitly linked to their specific source (transcript segment, regulatory article, or external publication), and several informant claims were independently cross-verified (for example, the Mayor's leadership framing, cross-checked against official municipal communications; and the historical existence of IIX Jogja, though not every specific transcript detail could be corroborated, such as the exact platform names cited as an illustrative quotation). On **transferability**, a single-case design inherently limits statistical generalizability; this study's international and domestic comparative analysis (Sections 3.7–3.8) was specifically designed to strengthen transferability by allowing readers to judge which aspects of Yogyakarta's findings appear locally specific (such as the heterogeneous-population complexity from its student and tourist concentration) and which appear to reflect broader structural patterns (such as the national digital-security pillar gap or the replicated SMKI regulatory pattern) — a strategy known in qualitative research literature as thick description.

Three specific data gaps most affect the strength of this study's conclusions: the absence of a direct DIY provincial government perspective, the absence of a City executive-leadership perspective, and the absence of student, elderly, and limited-digital-literacy citizen perspectives as distinct informant categories — the very groups most directly affected by, yet least represented in, this study's data. Finally, the research team's own institutional position — as members of a national civil-service training institute (IPDN) under the Ministry of Home Affairs, the same ministry that supervises local governments nationwide, including

Yogyakarta — is acknowledged as a factor potentially shaping how government informants framed their responses regarding institutional performance; this position offered methodological advantages (relatively easier field access, greater apparatus openness toward fellow government-affiliated researchers) alongside an acknowledged bias risk, one that should raise rather than lower confidence in findings that acknowledge institutional shortcomings, precisely because they were offered despite a structural tendency toward positive self-presentation.

5. Conclusion

This study examined how personal data protection governance is constructed in Yogyakarta City, a municipality operating at the intersection of Indonesia's national PDP mandate and its only constitutionally privileged regional autonomy regime. Across institutional structure, apparatus capacity, and sociopolitical dynamics, the evidence consistently characterizes Yogyakarta's governance pattern as substantive-partial compliance resting on a comparatively mature digital-governance foundation (an SPBE Index above the national average), yet without the complete formal structure the PDP Law requires — a gap concentrated sharply in four specific indicators (formal DPO designation, breach-notification SOP, dedicated PDP budget, and formal DIY-level coordination) rather than distributed evenly across the governance system. International and domestic comparison confirms this gap reflects a systemic-national and even a broader global implementation pattern, not a failure unique to Yogyakarta; Singapore and Malaysia needed over a decade to adopt DPO and notification standards Indonesia possessed from the outset, while Surakarta, Pekalongan, and Bantul Regency show the identical SMKI-without-PDP-specificity regulatory pattern found in Yogyakarta.

Theoretically, this pattern offers a tentative but distinctive nuance across four complementary frameworks: an inversion of the ceremonial-without-substance pattern dominant in institutional-compliance literature (institutional theory); evidence that frontline discretion can anticipate, rather than merely risk deviating from, formal regulation (street-level bureaucracy); evidence that collaborative capital

can be inherited across policy generations yet still require fresh institutional-design investment (collaborative governance); and evidence that organizational character can shift fluidly across policy domains under different leadership framing (political economy of bureaucracy).

Practically, the study's six-component Adaptive PDP Governance Model, together with its maturity-based prioritization and indicative quarterly roadmap, offers Yogyakarta City a concrete, evidence-grounded pathway that formalizes existing informal strengths rather than proposing an entirely new institutional architecture. For Indonesia's Ministry of Home Affairs, the domestic comparative findings suggest a specific, actionable opportunity: consolidating organically emerging good practices — particularly Bantul Regency's Information Security Committee model — into standardized technical guidance that could accelerate PDP-specific regulatory adoption nationally, much as existing SMKI/ISO 27001 guidance has already achieved for general information-security regulation.

This study's conclusions should be read as credible preliminary findings rather than definitive characterizations of Yogyakarta's PDP governance as a whole, given its reliance on a single primary data source and three unreached informant categories detailed in Section 4.6. Future research should prioritize completing triangulation with DIY provincial officials, City executive leadership, and — critically — the students, elderly residents, and limited-digital-literacy citizens whose interests this study's recommendations concern but whose voices this study's data does not directly capture; empirically testing the feasibility of Components 5 and 6 through dedicated consultation with Diskominfo, DIY provincial government, and the One Data Indonesia forum secretariat; and replicating this design across other Indonesian localities with special or distinct regional autonomy status — including Aceh and Papua — to test whether the "substance without formality" pattern is specific to Yogyakarta or generalizes to institutionally comparable regions.

6. References

- Almeida, V. A. F., Getschko, D., & Afonso, C. (2015). The origin and evolution of multistakeholder models. *IEEE Internet Computing*, 19(1), 74–79. <https://doi.org/10.1109/MIC.2015.15>
- Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543–571.
- Azam, N., Michala, L., Ansari, S., & Truong, N. B. (2023). Data privacy threat modelling for autonomous systems: A survey from the GDPR's perspective. *IEEE Transactions on Big Data*, 9(2), 388–414. <https://doi.org/10.1109/TBDATA.2022.3227336>
- Chatsuwana, K., et al. (2023). Personal data protection compliance assessment: A case study of government agencies. *Journal of Data Protection & Privacy*.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- DataGuidance. (2026). Thailand: Data protection overview.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of Public Administration Research and Theory*, 22(1), 1–29.
- Future of Privacy Forum. (2025). Global data protection law comparative tracker.
- Gao, B., Sun, J., & Wang, B. (2023). Personal information protection in government data openness using decision tree model. *Journal of Global Information Management*, 31(9). <https://doi.org/10.4018/JGIM.332815>
- He, M., & Chen, Y. (2025). Personal data protection in China: Progress, challenges and prospects in the age of big data and AI. *Telecommunications Policy*, 49(10). <https://doi.org/10.1016/j.telpol.2025.103076>
- InCountry. (2025). Malaysia Personal Data Protection Act (PDPA): Compliance guide.
- Jin, H., & Wang, L. (2025). Reassessing smart city development and personal data protection: A multi-stakeholder perspective. *Government Information Quarterly*.
- Kamm, L., Bogdanov, D., Brito, E., & Ostrak, A. (2024). Blueprints for deploying privacy enhancing technologies in e-government. *IFIP Advances in Information and Communication Technology*, 695, 3–19.
- Kane, G. C., Palmer, D., Phillips, A., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. *MIT Sloan Management Review*.
- Lipsky, M. (1980). *Street-level bureaucracy: Dilemmas of the individual in public services*. Russell Sage Foundation.
- Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385. <https://doi.org/10.1016/j.giq.2019.06.002>
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363. <https://doi.org/10.1086/226550>
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.
- Niskanen, W. A. (1971). *Bureaucracy and representative government*. Aldine-Atherton.
- Nnko, H., et al. (2026). Assessing the organisational readiness and compliance with personal data protection laws in Tanzania. *African Journal of Information Systems*.
- Sabatier, P. A., & Mazmanian, D. A. (1980). The implementation of public policy: A framework of analysis. *Policy Studies Journal*, 8(4), 538–560. <https://doi.org/10.1111/j.1541-0072.1980.tb01266.x>
- Scott, W. R. (2008). *Institutions and organizations: Ideas and interests* (3rd ed.). SAGE Publications.
- Securiti. (2025). China Personal Information Protection Law (PIPL): Compliance overview.
- VanBoskirk, S. (2016). Digital maturity model 5.0: Digital transformation playbook. Forrester Research.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, 28(2), 118–144. <https://doi.org/10.1016/j.jsis.2019.01.003>

Wilson, J. Q. (1989). *Bureaucracy: What government agencies do and why they do it*. Basic Books.

Yin, R. K. (2018). *Case study research and applications* (6th ed.). SAGE Publications.

Data sources and official documents: Badan Pusat Statistik. (2020). Hasil Sensus Penduduk 2020 (SP2020): Kota Yogyakarta; Badan Pusat Statistik Kota Yogyakarta. (2025). Yogyakarta Dalam Angka 2025; Dinas Kependudukan dan Pencatatan Sipil Kota Yogyakarta. (2025). Data Administrasi Kependudukan Kota Yogyakarta; Dinkominfo Kota Pekalongan. (2024). Kebijakan dan Sertifikasi Sistem Manajemen Keamanan Informasi (SMKI) Kota Pekalongan; Laboratorium Ilmu Pemerintahan UMY. (2023). Kajian Kewenangan Istimewa Daerah Istimewa Yogyakarta. Universitas Muhammadiyah Yogyakarta.

Legal instruments (Indonesia): Law No. 27/2022; Law No. 23/2014 on Regional Government; Presidential Regulation No. 95/2018 on the Electronic-Based Government System; Yogyakarta Regional Regulation No. 10/2021; Yogyakarta Mayoral Regulations No. 37/2023; Ministry of Home Affairs Regulation No. 17/2023.

7. Acknowledgements

This research was conducted under the 2026 Institutional Research (Lemlit) scheme of the Institut Pemerintahan Dalam Negeri (IPDN), Jatinangor, Indonesia. The authors thank all fourteen focus group discussion participants from Yogyakarta City's Diskominfo and Dindukcapil, and the citizen and industry representatives who contributed their time and perspectives to this study.

8. Author Declaration

The authors confirm that this work is original and has not been published elsewhere, in whole or in part. The authors declare no conflicts of interest. The lead research team's institutional affiliation with IPDN, under Indonesia's Ministry of Home Affairs, is disclosed in Section 4.6 as a factor considered in interpreting findings from government-affiliated informants. The focus group transcript underlying this study contains information that could identify participants and is therefore not publicly available; de-identified excerpts are available from the corresponding author upon reasonable request.