

**Harnessing Data for Democratic Development
in South and Southeast Asia” (D4DAsia)**

Country report for Indonesia

Draft

Executive Summary: Data Governance in Indonesia

Indonesia's data governance system has developed significantly over the past two decades. It has evolved from fragmented initiatives across ministries into a more coordinated national framework emphasizing transparency, interoperability, and digital transformation. The foundation lies in the 1945 Constitution, which guarantees citizens the right to obtain information and to have their personal data protected. This constitutional principle has been operationalized through a series of laws and regulations since the Reformasi era following 1998.

Policies that Increase Access to Data

The most important milestone for transparency is Law No. 14 of 2008 on Public Information Disclosure (Keterbukaan Informasi Publik or KIP Law). It gives citizens the right to access public information and requires every government agency to establish Information and Documentation Management Officers (PPID) responsible for handling information requests. The Central Information Commission (Komisi Informasi Pusat) acts as an oversight and dispute resolution body to ensure compliance and standardize disclosure procedures.

Indonesia is also a founding member of the Open Government Partnership (OGP), joined in 2011. The government further strengthened its data ecosystem through the One Data Indonesia (Satu Data Indonesia) policy under Presidential Regulation No. 39 of 2019, which promotes the use of standardized data formats, interoperability, and cross-agency coordination. This initiative complements Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik or SPBE), which formalized the framework for digital governance and data-driven public service.

The Central Statistics Agency (Badan Pusat Statistik or BPS) also plays a key role through Law No. 16 of 1997 on Statistics. It provides reliable official data and operates open data portals, such as bps.go.id, that offer national and regional datasets. Several subnational governments have launched similar open data platforms, including Jakarta, Bandung, Surabaya, and West Java, further expanding citizen access to public information.

Policies that Decrease Openness

While the overall policy direction favors transparency, several laws restrict access to data for reasons related to security, privacy, and national interest. Article 17 of the KIP Law defines categories of information exempt from disclosure, such as those related to national defense, law enforcement, diplomatic relations, and personal privacy. The Personal Data Protection Law (Law No. 27 of 2022) reinforces privacy rights but also permits broad exemptions for state institutions conducting activities in national defense, financial oversight, or law enforcement.

Other legal instruments, including Law No. 17 of 2011 on State Intelligence and Law No. 23 of 2006 on Demographic Administration (amended by Law No. 24 of 2013), provide further grounds for confidentiality. The creation of the National Data Center (NDC) through Presidential Regulation No. 132 of 2022 centralizes government data management, improving efficiency but limiting decentralized public access that had previously been available through multiple agency portals.

Data Protection and Privacy Framework

The enactment of the Personal Data Protection Law (PDP Law) in 2022 marked Indonesia's first comprehensive data protection regime. It aligns closely with global standards such as the EU General Data Protection Regulation (GDPR). The PDP Law establishes principles of legality, fairness,

transparency, purpose limitation, and accountability. It grants individuals the rights to access, rectify, erase, and transfer their personal data. The establishment of a Data Protection Authority (DPA) is under way, while interim oversight is carried out by the Ministry of Communication and Informatics (Kominfo).

Sectoral rules reinforce this framework. The Health Law of 2023, Bank Indonesia Regulation No. 3 of 2023, and the Financial Sector Development and Strengthening (P2SK) Law regulate the use of sensitive data in their respective areas. These measures strengthen privacy but also illustrate ongoing tension between data protection, administrative control, and economic governance.

Challenges and Recommendations

Despite these advances, Indonesia's data governance still faces fragmentation and uneven implementation. Many agencies maintain separate systems, and open data initiatives remain inconsistent. Bureaucratic reluctance, low digital literacy, and limited enforcement capacity hinder the realization of a unified data-sharing culture.

Key recommendations include:

- Strengthening coordination among ministries under the One Data Indonesia framework.
- Establishing the Data Protection Authority with clear enforcement powers.
- Improving data quality, interoperability, and digital infrastructure.
- Reviewing broad exemptions in security and privacy laws to ensure proportionality.
- Promoting a government culture that views information as a public right and disclosure as the default.

Indonesia has built a solid legal foundation for democratic and transparent data governance. The challenge ahead lies in translating laws into consistent practice. With sustained institutional reform, digital capacity building, and a stronger accountability framework, Indonesia can consolidate its role as a regional leader in open and inclusive data governance.

Introduction

This report on data governance in Indonesia is part of the “Harnessing Data for Democratic Development in South and Southeast Asia” (D4DAsia) project which aims, *inter alia*, to create and mobilize new knowledge about tensions, gaps, and the evolution of the data governance ecosystem taking into account formal and informal policies and practices.

In today's digital age, data governance ecosystems play a crucial role in shaping our societies. These ecosystems, comprising policies, laws, practices, behaviours, and technologies, aim to govern data in ways that protect rights, foster innovation, enhance transparency, and ultimately promote democratic and inclusive governance. However, the landscape of data governance is complex and often fraught with challenges, particularly in South and Southeast Asia.

Data governance ecosystems are made up of policies, laws, practices, behaviours, and technologies that govern data. An ideal data governance system would protect rights, enable innovation, improve transparency, and help in bringing about democratic, inclusive governance. Through the rest of the report, unless the context indicates otherwise, the term “policies” is used as shorthand for policies, statutes, regulations, rules, administrative orders, and even practices and technologies that are used to implement all of those as part of the data governance ecosystems.

Data is increasingly being recognised as an enabler for development. It is an essential requirement for policy making and monitoring of development goals and targets. When effectively managed, data can be used as an asset to support significant development actions such as poverty reduction, food security, mitigating impact of climate change, and disaster management. If mismanaged, it can exacerbate inequalities and undermine the development potential of the same actions.

The D4DAsia project has produced nine reports so far, seven detailed individual country reports which deal with the issues of data governance in the following countries: India, Indonesia, Nepal, Pakistan, Philippines, Sri Lanka and Thailand; a detailed look at data protection in South Korea; and a synthesis report that summarizes the findings from the various countries while drawing out the contrasts amongst them, along with detailed findings to the research questions we'd posed, which were:

1. What is common, and what is nationally specific, in the emerging data governance architectures in South and Southeast Asia? What are the explanations?

2. What are the implications of the emergent nature of the governance architecture? Because there is no overall design that envisions how the parts fit together, it is likely that there will be friction points and even contradictions. How are these being worked out?
3. The emerging governance architecture involves trade-offs among objectives such as greater accountability of powerholders, economic growth including creation of employment and wealth, resilience of systems, etc. How have different societies: (a) explicitly recognized the trade-offs or not; and (b) handled them?
4. Are there legislative or policy innovations with potential for replication? What are the modalities of sharing experiences? Are developing countries learning from each other, or are they learning from the developed countries?
5. How were the laws and bills developed? What expertise was brought to bear? How open were the procedures? How receptive were drafters to suggestions and criticisms?
6. How were capacity challenges addressed: by simplifying the laws or by tolerating incomplete implementation?

Structure of the report

1. Governance Background

This report begins by outlining the constitutional and governance framework that underpins Indonesia's legal and policy environment. Understanding how the state allocates, delegates, and exercises lawmaking powers is essential for contextualizing Indonesia's approach to data governance, privacy, and digital openness.

1.1 Constitutional and Institutional Framework

Indonesia's 1945 Constitution (*Undang-Undang Dasar Negara Republik Indonesia Tahun 1945* or "UUD 1945") establishes a presidential system with a separation of powers among the executive, legislative, and judicial branches. The President serves as both Head of State and Head of Government, wielding substantial authority in policy formulation and execution, including the issuance of government regulations and presidential decrees that often operationalize legislative mandates.¹

The People's Consultative Assembly (Majelis Permusyawaratan Rakyat – MPR) holds the highest constitutional authority, although its role today is largely symbolic and normative after the post-1999 constitutional amendments. The House of Representatives (Dewan Perwakilan Rakyat– DPR) and the Regional Representative Council (Dewan Perwakilan Daerah– DPD) together exercise legislative powers. The DPR drafts and enacts laws jointly with the President, while the DPD represents regional interests in legislative deliberations.²

The judiciary, comprising the Supreme Court (Mahkamah Agung) and the Constitutional Court (Mahkamah Konstitusi), plays a critical role in ensuring constitutional supremacy and safeguarding individual rights. The Constitutional Court has the power to review laws (judicial review) against the Constitution, thereby providing a mechanism to overturn or invalidate legislation or regulations inconsistent with constitutional guarantees.³ The Supreme Court also reviews the legality of subordinate regulations (*peraturan di bawah undang-undang*), ensuring the coherence of Indonesia's normative hierarchy (*tata urutan peraturan perundang-undangan*).⁴

1.2 Lawmaking and Delegation of Powers

Under the Law No. 12 of 2011 (as amended by Law No. 13 of 2022) on the Formation of Laws and Regulations, Indonesia's legal system follows a hierarchical order of norms (*stufenbau theory*). The hierarchy, beginning from the Constitution, followed by Laws (*Undang-Undang*), Government Regulations (*Peraturan Pemerintah*), Presidential Regulations (*Peraturan Presiden*), and Regional Regulations (*Peraturan Daerah*), ensures that lower-level instruments must align with higher-level laws.⁵

In practice, this structure enables the executive branch, particularly the President and ministries, to issue implementing regulations that detail and operationalize legislative provisions. This delegation of regulatory authority is vital for the execution of complex and technical domains such as data governance, digital transformation, and cybersecurity. The Ministry of Communication and Informatics (Kementerian Komunikasi dan Informatika – MOCI) plays a central role in drafting and enforcing regulations governing data protection, open data, and digital ecosystems.⁶

1.3 Role of the Judiciary and Policy Enforcement

² Butt, Simon & Lindsey, Tim. *The Constitution of Indonesia: A Contextual Analysis*. Hart Publishing, 2012.

³ Mahkamah Konstitusi Republik Indonesia. "Putusan Nomor 5/PUU-V/2007" (Case on Judicial Review Mechanism).

Draft

⁴ Law No. 12 of 2011 (as amended by Law No. 13 of 2022) on the Formation of Laws and Regulations (*Pembentukan Peraturan Perundang-Undangan*).

⁵ Strong, C. F. *Modern Political Constitutions*. Methuen & Co. Ltd, 1973.

⁶ Ministry of Communication and Informatics (MOCI). "Digital Transformation Roadmap 2021–2024." Jakarta, 2021.

In addition to lawmaking, the judiciary safeguards both procedural and substantive legality in public policy. The Constitutional Court regularly adjudicates cases related to the freedom of information, privacy, and constitutional rights in the digital sphere, for instance, reviewing the legality of electronic information and transaction laws or surveillance powers.⁷ This judicial oversight provides the necessary constitutional checks on executive or legislative overreach, ensuring that digital governance frameworks remain anchored in human rights and rule-of-law principles.

Moreover, law enforcement and administrative agencies, such as the Ombudsman of the Republic of Indonesia and the National Commission on Human Rights (Komnas HAM), contribute to oversight by ensuring the accountability of public institutions, including those involved in digital and data governance.

1.4 Legal and Regulatory Background for Data Governance

Indonesia's governance landscape has evolved significantly over the past two decades, especially with the growing prominence of the digital economy, data-driven policymaking, and cross-border data flows. Early frameworks, such as Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) and its amendment through Law No. 19 of 2016, laid the groundwork for regulating electronic systems, digital contracts, and online interactions. Subsequent regulations, such as Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions (GR 71/2019), further clarified the responsibilities of electronic system operators (*penyelenggara sistem elektronik*), including obligations for data protection and security.

These frameworks culminated in the Personal Data Protection Law (Law No. 27 of 2022), marking Indonesia's first comprehensive legal instrument governing personal data processing. Together, these laws represent Indonesia's gradual shift from fragmented sectoral governance to a unified national framework for data protection, interoperability, and responsible data use.⁸

The overall governance environment therefore shapes how Indonesia approaches data openness, privacy, and access, balancing constitutional guarantees, executive authority, judicial oversight, and sectoral regulation in the broader quest to develop a trusted, rights-based, and innovation-friendly data ecosystem.

Draft

⁷ Mahkamah Konstitusi Decisions related to Law No. 11/2008 on Electronic Information and Transactions, e.g., *Putusan No. 50/PUU-VI/2008*.

⁸ Simandjuntak, D. et al. "Indonesia's Data Governance Framework: From Fragmentation to Integration." *Journal of Southeast Asian Public Policy*, Vol. 8 (2), 2023.

**Harnessing Data for Democratic Development
in South and Southeast Asia (D4DAsia) project
Country Report for Indonesia**

Author: Ibrahim Kholilul Rohman

0. Background

1. Legal Foundation

Indonesia's legal and constitutional framework is founded on the 1945 Constitution of the Republic of Indonesia (Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, UUD 1945), which has undergone several amendments, particularly following the fall of the Suharto regime in 1998. As a unitary state, Indonesia is governed as a single entity under a centralized authority, while regional governments exercise limited autonomy based on powers delegated by the central government. The state adopts a separation of powers among the executive, legislative, and judicial branches.

The President, elected directly by the people, serves as both Head of State and Head of Government, while legislative authority rests with the People's Consultative Assembly (Majelis Permusyawaratan Rakyat, MPR), comprising the Regional Representative Council (Dewan Perwakilan Daerah, DPD) and the House of Representatives (Dewan Perwakilan Rakyat, DPR). The judiciary operates independently, with the Supreme Court (Mahkamah Agung) serving as the highest judicial authority and the Constitutional Court (Mahkamah Konstitusi) empowered to

review legislation to ensure conformity with the Constitution (Butt & Lindsey, 2018; Crouch, 2010).

Indonesia's legal system follows the civil law tradition, heavily influenced by Dutch colonial law, customary (*adat*) law, and Islamic law (Lev, 1972; Pompe, 2005). Statutory law serves as the primary source of law, encompassing acts enacted by the legislature and regulations issued by the executive branch. *Adat* law remains significant in rural and traditional communities, while Islamic law applies primarily to personal and family matters among Muslim citizens. Since the late 1990s, Indonesia has implemented a policy of decentralization, granting greater authority to regional governments to enhance democratic accountability and local service delivery (World Bank, 2003; Hofman & Kaiser, 2004). Nonetheless, the central government retains control over key sectors such as defense, foreign affairs, and fiscal policy. This governance model seeks to balance central authority with regional autonomy, ensuring that legislation and policy remain consistent with constitutional principles (Crouch, 2010; Lindsey, 2008).

In the absence of proper data governance, risks such as data loss, leakage, and misuse may emerge, leading to institutional, legal, and societal challenges (Bannister & Connolly, 2014). Accordingly, it is essential to establish clear data management policies and ensure shared responsibility among all stakeholders, including public institutions, private entities, and individuals. Indonesia's data governance framework incorporates strategies for managing data operations, such as preservation, curation, accessibility, and quality, while addressing legal, policy, and institutional dimensions (BPS, 2022; Ministry of Communication and Informatics, 2023).

The constitutional foundation for data governance and protection in Indonesia can be traced to the 1945 Constitution, which explicitly guarantees that *“every individual has the right to communicate and to obtain information for the development of their personal and social environment.”* Furthermore, Article 28G(1) affirms that *“every person has the right to protection of themselves, their family, honor, dignity, and property, and has the right to a sense of security and protection from threats that may compel them to do or refrain from doing something.”* These provisions form the legal basis for recognizing the right to information and data privacy as integral components of human rights in Indonesia (Butt & Lindsey, 2018; Setiadi, 2022).

Data governance in Indonesia entails the establishment of a comprehensive framework of laws, policies, and technical standards to manage data across the public sector. This framework addresses data management, utilization, security, integrity, and accuracy, ensuring that digital technologies reliant on large volumes of data are implemented securely and in accordance with existing regulations. Effective data governance is essential to ensuring the usability, reliability, and protection of data, thereby supporting sustainable development objectives and mitigating risks such as data breaches, reputational damage, and financial losses (OECD, 2022; ASEAN, 2021).

A significant milestone in Indonesia's transparency and data governance agenda was the Public Information Disclosure Act (Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik/UU KIP), enacted in 2008 and effective as of 1 May 2010. Commonly referred to as the Right to Information (RTI) Law, it was designed to empower citizens by providing a legal right to access and obtain public information (Sagala, 2013; Paramita, 2020). This legislation represents a critical component of the post-1998 reform era,⁹ aimed at institutionalizing transparency and accountability following the fall of the authoritarian *New Order* regime (Liddle, 2019). Prior to its enactment, Indonesia's policy-making process was characterized by limited public participation, minimal transparency, and restricted access to information,¹⁰ often resulting in policies whose targets and outcomes lacked accuracy and accountability (Hadiwinata, 2003). The RTI Law sought to address these deficiencies by promoting open governance and strengthening public oversight through access to information (OECD, 2021).

Indonesia's commitment to transparency and accountability is thus reflected in legislative mandates such as Law No. 14 of 2008 on Public Information Disclosure (RTI Law), which ensures citizens' rights to request, obtain, and disseminate public

⁹ Azizah Saffa, "Indonesia Advancing Digitalisation in Public Service Delivery," OpenGov, June 6, 2023, <https://opengovasia.com/indonesia-advancing-digitalisation-in-public-service-delivery/>.

¹⁰ Indonesia officially embraced the Public Information Disclosure Act (RTI Act) in 2008, and it became effective on 1 May 2010. The genesis of this legislation traces back to the year 2000 when the Indonesian Center for Environmental Law (ICEL) spearheaded the initiative. This effort garnered support from a diverse coalition of around 40 civil society organizations and individuals. The Coalition formulated a preliminary law draft in 2002, serving as the foundation for the subsequent legislative proposal crafted by the Parliamentary Special Committee. This proposal was then submitted to then-President Megawati Sukarnoputri. However, negotiations encountered a hiatus lasting several years before recommencing in 2005. In addition to the RTI Act, supplementary regulations, including the Government Regulation on the Implementation of Freedom of Information Act and the Central Information Commission Regulation on Public Information Service Standards, were later enacted to complement and elucidate the provisions of the law. <https://www.article19.org/resources/country-report-the-right-to-information-in-indonesia/>

information.¹¹ The law emphasizes public participation,¹² transparent governance, and effective information management by public institutions.¹³ Establishing information and documentation systems is a core requirement of this framework to facilitate access and uphold the principles of good governance (Komisi Informasi Pusat, 2023). While this legislation provides a solid foundation for Indonesia's evolving data governance architecture, emerging technological and institutional challenges continue to test the consistency and effectiveness of its implementation (UNESCAP, 2023; ASEAN Digital Governance Report, 2022).

1.1. Indonesia's Data Governance Landscape

Indonesia's data governance framework has evolved substantially since its early conception, guided by key legislative milestones that have progressively shaped its regulatory and institutional landscape. Foundationally, Article 28F of the 1945 Constitution guarantees every individual the right to communicate and obtain information for personal and societal development.¹⁴ This constitutional principle was further institutionalized through Law No. 14 of 2008 on Public Information Disclosure (Undang-Undang Keterbukaan Informasi Publik, UU KIP), Indonesia's Right to Information (RTI) Law, which marked a turning point in the nation's commitment to transparency and accountability following the 1998 *Reformasi* movement.¹⁵

Complementing the RTI framework, other pivotal legislations include Law No. 39 of 1999 on Human Rights, Law No. 25 of 2004 on the National Development Planning System, and Presidential Regulation No. 39 of 2019 on One Data Indonesia (Satu Data Indonesia). Together, these laws underscore a coherent policy direction: to ensure data openness, interoperability, and reliability in public decision-making.¹⁶

Effective data governance requires that both public and private entities possess the capacity to make informed, accountable, and legally compliant decisions regarding

¹¹ Mendel, Toby, Notess, Laura. 2022. *The right to information in times of crisis: access to information – saving lives, building trust, bringing hope!*. UNESCO:France. Page 2.

¹² Simon Butt, Freedom of Information Law and its Application in Indonesia: A Preliminary Assessment, (2014) ASJCL p 113-154

¹³ Sakapurnama, Eko and Safitri, Nurul (2013) "Good Governance Aspect in Implementation of The Transparency of Public Information Law," BSNIS & BIROKRASI: Jurnal Ilmu Administrasi dan Organisasi: Vol. 18 : No. 3 , Article 8. DOI: Law No. 14 of 2008 on Disclosure of Public Information, art. 3. 10.20476/jbb.v19i1.1879 Available at: <https://scholarhub.ui.ac.id/jbb/vol18/iss3/8>. Page 71.

¹⁴ Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Article 28F.

¹⁵ Law No. 14 of 2008 on Public Information Disclosure (UU KIP); Winastwan Gora Swajati, *Kajian Kebijakan dan Sistem Pengelolaan Data Penelitian Indonesia*, Bappenas, p. 19.

¹⁶ Government of the Republic of Indonesia, Cabinet Secretariat. 2019. President Jokowi Issues Regulation on One-Data Indonesia, 27 June. <https://setkab.go.id/en/president-jokowi-issues-regulation-on-satu-data-indonesia/>; United Nations Resident Coordination Office. 2021. Situation Analysis of the State of Data in Indonesia. UNRCO Jakarta, p. 11.

data use, value creation, and risk management. For a country as large and complex as Indonesia, this necessitates a structured governance system capable of minimizing fragmentation and ensuring that principles of transparency translate into enforceable practices.¹⁷

This report, therefore, highlights five key dimensions of Indonesia's evolving data governance ecosystem: (1) the institutionalization of transparency through the 2008 RTI Law; (2) the catalytic role of Indonesia's participation in the Open Government Partnership (OGP) since 2011 in advancing open data systems; (3) the coexistence of policies that both promote and restrict data openness; (4) the persistent gap between normative aspirations and implementation; and (5) sectoral best practices in data management, particularly in health and finance, that gained prominence during the pandemic¹⁸

2. In the “Laws that Open Access” Section

2.1. Law No. 14 of 2008 on Public Information Disclosure (Right to Information Law)

The Law No. 14 of 2008 on Public Information Disclosure (UU KIP), enacted on 30 April 2008, represents a significant milestone in Indonesia's democratic evolution and its data governance architecture. As Indonesia's Right to Information (RTI) legislation, it codifies citizens' rights to access public information and sets forth detailed obligations for government agencies to disclose information both reactively and proactively.¹⁹ The law formally entered into effect in 2010, following a two-year preparatory period for institutional implementation (Mendel, 2008).

Article 2 (1) of the law explicitly provides that *“all public information shall be open and accessible to users of public information, which includes Indonesian citizens and legal entities. All citizens and entities possess the right to request, view, understand, and obtain copies of and distribute public information.”* Article 3 further delineates these rights, emphasizing the public's entitlement to access, comprehend, and monitor policymaking processes, programs, and decision-making. These provisions underscore that access to information is not merely a procedural right but a substantive democratic entitlement, a precondition for meaningful participation and accountability.

The law classifies public information into three categories to be disclosed:

¹⁷ Asian Development Bank. Data Management Policies and Strategies for Government (2021); World Economic Forum. Articulating Value from Data (2021).

¹⁸ Open Government Indonesia. 2022. *Indonesia Open Government Partnership National Action Plan 2023–2024*, Bappenas: Jakarta, p. 1; Raviyo Patra. 2020. *Independent Reporting Mechanism (IRM): Indonesia Design Report 2018–2020*. The Open Government Partnership, Jakarta, p. 10.

¹⁹ Law No. 14 of 2008, art. 7 (1) & (2)

- Periodically, covering reports on institutional activities, performance, and financial management;
- Immediately, including information that could affect public safety and order; and
- At any time, it comprises documents such as agency policies, decisions and their rationales, work plans, annual budgets, and reports on public information service performance.

In operational terms, the RTI Law imposes extensive obligations on public authorities to establish information and documentation management systems (Pejabat Pengelola Informasi dan Dokumentasi, PPID) responsible for processing and publishing information. These systems are designed to ensure consistent transparency, encourage public participation, and enhance the quality of governance.²⁰ The law envisions transparency not merely as administrative compliance but as an enabler of scientific development, civic engagement, and policy accountability (Setiyono & McLeod, 2010; Nurhasim & Wicaksono, 2016).

To support implementation, the law created the Central Information Commission (Komisi Informasi Pusat), an independent body mandated to formulate technical standards for information services and adjudicate public information disputes. This body issued Regulation No. 1/2010 on Standard Public Information Services, which outlines minimum service standards for disclosure practices across public institutions. The Commission also provides non-litigious mechanisms, mediation and adjudication, for resolving access disputes, thereby institutionalizing citizens' right to information through an accessible administrative process.

Conceptually, the RTI framework redefines the relationship between the state and the citizen by embedding transparency as a constitutional principle.²¹ It aligns Indonesia's governance framework with broader global trends emphasizing open data, civic participation, and human rights-based approaches to information access (Banisar, 2006; Mendel, 2008; Fox, 2007). In this sense, Law No. 14 of 2008 serves not only as a transparency instrument but also as a foundational component of Indonesia's data governance ecosystem, one that supports trust, accountability, and evidence-based policymaking.

²⁰ Sakapurnama, Eko and Safitri, Nurul (2013) "Good Governance Aspect in Implementation of The Transparency of Public Information Law," *BISNIS & BIROKRASI: Jurnal Ilmu Administrasi dan Organisasi*: Vol. 18 : No. 3 , Article 8. DOI: 10.20476/jbb.v19i1.1879 Available at: <https://scholarhub.ui.ac.id/jbb/vol18/iss3/8>. Page 71.

²¹ [Mendel, Toby, Notess, Laura](#). 2022. *The right to information in times of crisis: access to information – saving lives, building trust, bringing hope!*. UNESCO:France. Page 2.

While the enactment of Law No. 14 of 2008 on Public Information Disclosure (UU KIP) represents a significant milestone in Indonesia's democratization process, the true test of its impact lies in the effective implementation of transparency standards across public institutions. The law's success cannot be gauged solely by its existence as a legislative instrument but by the extent to which it translates into practical and enforceable rights for citizens.²² Genuine government accountability requires that violations of the right to information be subject to clear remedies, enabling citizens to challenge opacity and compel disclosure through established mechanisms such as the Information Commission.

In the longer term, however, the effectiveness of UU KIP depends not merely on legal enforcement but on the institutionalization of a culture of openness and accountability within the public sector. Sustainable transparency emerges when state institutions internalize the principle that information belongs to the public and that disclosure is the norm rather than the exception. Such a transformation demands not only regulatory compliance but also normative change, a shift in bureaucratic behavior driven by the recognition of citizens as rights-holders rather than passive recipients of government information (Fox, 2007; McGee & Gaventa, 2011).

2.2. Open Government and the One Data Indonesia Initiative

Indonesia's commitment to transparency and data openness has evolved through a series of institutional and policy initiatives aimed at fostering accountability and participatory governance. Following the enactment of Law No. 14 of 2008 on Public Information Disclosure (UU KIP), which laid the legal foundation for citizens' right to access information, Indonesia advanced its transparency agenda through multilateral and national frameworks that promote open government and data-driven policymaking.

In 2011, Indonesia became one of the founding members of the Open Government Partnership (OGP), a global initiative that promotes transparent, participatory, and accountable governance. Through successive National Action Plans (Rencana Aksi Nasional, RAN), Indonesia has sought to strengthen public participation, improve access to government information, and enhance integrity in public service delivery.²³ The OGP process also

²² Azizah Saffa, "Indonesia Advancing Digitalisation in Public Service Delivery," OpenGov, June 6, 2023, <https://opengovasia.com/indonesia-advancing-digitalisation-in-public-service-delivery/>.

²³ Ravio Patra. (2020). *Independent Reporting Mechanism (IRM): Indonesia Design Report 2018–2020*. The Open Government Partnership. Jakarta, p. 10.

positioned Indonesia as a regional leader in promoting open data as a mechanism for innovation, civic engagement, and anti-corruption reform.²⁴

Building on this momentum, the government launched the One Data Indonesia (Satu Data Indonesia, ODI) initiative, formally institutionalized through Presidential Regulation No. 39 of 2019.²⁵ The ODI framework aims to harmonize and standardize data governance across public institutions by ensuring interoperability, data quality, and accessibility. It establishes principles for data management that include the use of common standards, metadata, and reference codes, thereby promoting the production and utilization of accurate, integrated, and accountable data across both central and regional agencies.²⁶

Together, the OGP and ODI initiatives represent a critical evolution in Indonesia's data governance landscape, from a rights-based approach emphasizing public access to information, toward a systemic and coordinated approach to data interoperability and governance. These frameworks not only facilitate transparency and evidence-based policymaking but also enable cross-sectoral collaboration and digital transformation in public administration.²⁷

This legislation brought about a significant paradigm shift. Previously, government data in Indonesia was *closed by default* and only made public upon request; under the new framework, it became *open by default* and is now mandated to be accessible and available to all citizens.²⁸ Under this policy regime, Indonesia established two key institutional mechanisms: (a) a **Steering Council (SC)**, comprising ministers responsible for strategic

²⁴ Open Government Indonesia. (2022). *Indonesia Open Government Partnership National Action Plan 2023–2024*. Bappenas: Jakarta, p. 1.

²⁵ Government of the Republic of Indonesia, Cabinet Secretariat. (2019). *President Jokowi Issues Regulation on One-Data Indonesia*. 27 June. <https://setkab.go.id/en/president-jokowi-issues-regulation-on-satu-data-indonesia/>

²⁶ Winastwan Gora Swajati. *Kajian Kebijakan dan Sistem Pengelolaan Data Penelitian Indonesia*. Bappenas, p. 19; Sekretariat Nasional Open Government Indonesia. *The Role of Satu Data Indonesia to Propel the Practices of Open Government*.

<https://ogi.bappenas.go.id/storage/files/news/licnnCihfGkp8SSOQTdRdlo8jZReMOg5bXuEo2o.pdf>

²⁷ World Bank. *Open Data Brings Change to Indonesia*; World Bank. *Indonesia's Government and Civil Society in Partnership to Encourage Greater Data Transparency*; United Nations Resident Coordination Office. (2021). *Situation Analysis of the State of Data in Indonesia*. UNRCO Jakarta, p. 11; Asian Development Bank. (2022). *Data Management Policies and Strategies for Government*.

<https://www.adb.org/sites/default/files/publication/849541/data-management-policies-strategies-government.pdf>; World Economic Forum. (2021). *Articulating Value from Data*.

²⁸ Government of the Republic of Indonesia, Cabinet Secretariat. 2019. *President Jokowi Issues Regulation on One-Data Indonesia*. 27 June. <https://setkab.go.id/en/president-jokowi-issues-regulation-on-satu-data-indonesia/>; World Bank. *Open Data Brings Change to Indonesia*; Sekretariat Nasional Open Government Indonesia. *The Role of Satu Data Indonesia to Propel the Practices of Open Government*. <https://ogi.bappenas.go.id/storage/files/news/licnnCihfGkp8SSOQTdRdlo8jZReMOg5bXuEo2o.pdf>

sectors, tasked with coordinating policies, monitoring, evaluating, and reporting the progress of the **One Data Indonesia (Satu Data Indonesia)** initiative; and (b) **Central Data Trustees (CDT)**, mandated to formulate data standards, define metadata structures, provide policy recommendations, and support implementation efforts.²⁹ Through **Ministerial Decree Number 31/M.PPN/HK/04/2021** concerning the Establishment of the Working Group for the Central-Level Indonesian One Data Forum, these functional units were formally institutionalized.³⁰

2.3. Census Act (Law No. 16 of 1997 on Statistics)

The Law No. 16 of 1997 on Statistics, commonly referred to as the Census Act, serves as the foundational legal framework for statistical governance and data management in Indonesia. The law was enacted to establish a National Statistical System (NSS) that ensures the production and use of reliable, accurate, and timely statistical data to support evidence-based policymaking and national development planning.³¹ It defines statistics as “*data obtained by collection, preparation, presentation, and analysis*” and introduces a systematic approach to regulating the relationship among various statistical actors and activities across government institutions.³²

Under this law, the Central Statistics Agency (Badan Pusat Statistik, or BPS) is designated as the main authority responsible for conducting statistical activities at the national level. These activities include:

- Censuses, carried out at least once every ten years, consisting of a Population Census, an Agricultural Census, and an Economic Census;
- Surveys, conducted periodically or as needed to obtain more detailed or thematic data;
- Intercensal Surveys, implemented to bridge information gaps between census years; and

²⁹ Winastwan Gora Swajati. *Kajian Kebijakan dan Sistem Pengelolaan Data Penelitian Indonesia*. Bappenas, p. 19; United Nations Resident Coordination Office. 2021. *Situation Analysis of the State of Data in Indonesia*. UNRCO Jakarta, p. 11.

³⁰ Open Government Indonesia. 2022. *Indonesia Open Government Partnership National Action Plan 2023–2024*. Bappenas: Jakarta, p. 1; Rasio Patra. 2020. *Independent Reporting Mechanism (IRM): Indonesia Design Report 2018–2020*. The Open Government Partnership, Jakarta, p. 10.

³¹ Law of the Republic of Indonesia No. 16 of 1997 on Statistics (*Undang-Undang Republik Indonesia Nomor 16 Tahun 1997 tentang Statistik*), Preamble and Article 1.

³² Winastwan Gora Swajati. *Kajian Kebijakan dan Sistem Pengelolaan Data Penelitian Indonesia*. Bappenas, p. 19.

- Compilation of Administrative Records, which utilizes data from administrative documents maintained by government and non-government entities.³³

The Census Act outlines that statistical activities must serve four key purposes:

- a. to support national development;
- b. to strengthen a reliable, effective, and efficient National Statistical System;
- c. to enhance public awareness regarding the importance and role of statistics; and
- d. to support the advancement of science and technology.³⁴

Importantly, the Act also introduces a principle of openness in data access, stipulating that statistical data, unless restricted by specific legislation, should be publicly accessible and disseminated in the Official Statistics News (*Berita Resmi Statistik*) or through BPS offices at the national, provincial, and local levels.³⁵ This provision aligns with the country's broader transparency framework as embodied in the Law No. 14 of 2008 on Public Information Disclosure (UU KIP), reinforcing data as a public good to be utilized for research, policy evaluation, and societal benefit³⁶

In practice, BPS has operationalized these principles through its open data portal, accessible via <https://www.bps.go.id>, which serves as a centralized hub for disseminating official statistics. The portal represents a significant institutional effort toward improving data interoperability, accessibility, and public participation in statistical use and analysis. As noted in the United Nations Resident Coordination Office (UNRCO) Situation Analysis (2021), this approach contributes to strengthening Indonesia's data ecosystem and supporting policy coherence across sectors.³⁷

3. Openness / Increasing Access

3.1. Open Data, Laws, Policies, and Practices

The Government of Indonesia (GOI) has demonstrated sustained commitment to advancing digital governance and data-driven policymaking. The foundation of this commitment can be traced to Law Number 25 of 2004 on the National Development Planning System, particularly Article 31, which mandates that national development

³³ Law No. 16/1997, Articles 7–10; Central Statistics Agency (BPS). *Indonesia Census Framework and Implementation Guidelines*.

³⁴ Law No. 16/1997, Article 3

³⁵ Law No. 16/1997, Articles 11–13; Government of Indonesia, Cabinet Secretariat. 2019. *President Jokowi Issues Regulation on One Data Indonesia*, June 27.

³⁶ World Bank. *Open Data Brings Change to Indonesia*.

³⁷ United Nations Resident Coordination Office (UNRCO). 2021. *Situation Analysis of the State of Data in Indonesia*, p. 11.

planning be based on accurate, reliable, and transparent data. This law positioned data not merely as a technical input but as a strategic national asset, central to evidence-based policy formulation and public accountability.³⁸

Despite this mandate, the early phases of Indonesia's e-governance (2004–2018) were characterized by fragmented digital systems, siloed databases, and limited inter-agency coordination. Various ministries and local governments launched electronic service platforms, commonly referred to as *e-services*, that often operated independently, lacked interoperability, and faced sustainability challenges³⁹ This fragmentation hindered the realization of an integrated “whole-of-government” data ecosystem that could support open data access and coordinated digital services.

3.1.1. Presidential Regulation No. 95 of 2018 on Electronic-Based Government System (SPBE)

A major policy breakthrough came with the enactment of Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik, or SPBE).⁴⁰ This regulation formalized the framework for digital transformation in public administration, setting out principles for data management, interoperability, information security, and public service integration. The SPBE aims to strengthen coordination across ministries and agencies, streamline data standards, and improve service delivery through data-driven decision-making.

Article 13 of this regulation establishes specific mandates regarding data governance, including the establishment of a national data center, uniform metadata standards, and audit mechanisms for information integrity. It further mandates that government entities manage data with due consideration for confidentiality, availability, and integrity, introducing for the first time a comprehensive regime for digital risk management and protection of classified information.⁴¹

The SPBE architecture also underpins Indonesia's open data platforms at both national and subnational levels. The national open data portal, <https://data.go.id>, serves as the primary interface for citizens to access government datasets.⁴² Several local governments have also developed regional portals, reflecting a decentralized

³⁸ Law No. 25 of 2004 on the National Development Planning System.

³⁹ World Bank. (2017). *Indonesia: E-Government Review*. Washington, DC.

⁴⁰ Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System (SPBE).

⁴¹ Kominfo. (2020). *SPBE Implementation Framework*.

⁴² Open Data Indonesia Portal – <https://data.go.id>.

model of open data implementation—for example, the West Java Province Open Data Portal (<https://opendata.jabarprov.go.id>), Jakarta Province’s One Data Portal (<https://satudata.jakarta.go.id>), Bandung City Open Data Portal (<https://opendata.bandung.go.id>), and Surabaya City Open Data Portal (<https://opendata.surabaya.go.id>).⁴³ The Central Statistics Agency (Badan Pusat Statistik, BPS) also publishes comprehensive datasets through its official statistics portal, integrating statistical outputs with open data infrastructure.⁴⁴

3.1.2. Fragmentation and Governance Challenges

While the SPBE marked a decisive shift toward unified and interoperable governance, institutional fragmentation persisted. A study by the Ministry of Administrative and Bureaucratic Reform (KemenPANRB, 2018) found that many agencies continued to operate under divergent data standards and lacked a unified e-government policy framework.⁴⁵ The report noted that these challenges stemmed from the absence of consistent leadership in data governance, uneven digital infrastructure, and limited capacity in data literacy among public officials.

Recognizing this, President Joko Widodo, in his address during the People’s Consultative Assembly (MPR) Annual Session and the Joint Session of the DPR and DPD in August 2021, underscored the need for government decision-making to be grounded in data, science, and technology.⁴⁶ This statement reaffirmed Indonesia’s commitment to institutionalizing a data-driven governance culture, one that ensures transparency, efficiency, and accountability in the public sector.

3.1.3 Balancing Openness and Protection

The increasing digitization of public administration has elevated the significance of data governance as both a transparency and security imperative. Open data is now recognized as a fundamental right and an essential component of democratic governance, reinforcing citizens’ access to public information. However, the proliferation of “mega datasets” in the digital era also brings heightened risks of privacy breaches, data misuse, and cyber vulnerabilities.⁴⁷

⁴³ Regional Open Data Portals (West Java, Jakarta, Bandung, Surabaya).

⁴⁴ Badan Pusat Statistik (BPS) – <https://www.bps.go.id>.

⁴⁵ KemenPANRB. (2018). *Evaluasi SPBE Nasional*.

⁴⁶ President Joko Widodo’s Speech at the Annual MPR Session, 16 August 2021.

⁴⁷ OECD (2020). *Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact*. Paris: OECD Publishing.

The GOI has sought to address these challenges through laws emphasizing the protection of personal data and information security. As digital adoption accelerated in the 1990s and 2000s, data protection began to be treated as an extension of human rights, culminating in recent legislative measures such as Law No. 27 of 2022 on Personal Data Protection (PDP Law), which formalizes the right to informational privacy.⁴⁸

Yet, practical implementation remains uneven. Studies on Right to Information (RTI) and proactive disclosure laws in Indonesia reveal gaps between legal provisions and actual practice.⁴⁹ Although the Public Information Disclosure Act (Law No. 14 of 2008) and various cabinet resolutions require agencies to publish key information online, compliance is inconsistent due to limited technical capacity, outdated data management systems, and lack of enforcement mechanisms.⁵⁰

Consequently, while Indonesia's policy architecture has evolved significantly toward openness and interoperability, the challenge now lies in ensuring that open data policies translate into sustained institutional practices, supported by skilled human resources, robust infrastructure, and coherent regulatory enforcement.

4. Proactive

4.1. Right to Information and Proactive Disclosure

Proactive disclosure is a central feature of Indonesia's Law No. 14 of 2008 on Public Information Disclosure (*Undang-Undang Keterbukaan Informasi Publik* or "KIP Law"), which establishes the legal framework for public access to information held by government institutions. The KIP Law mandates every public body (*badan publik*) to actively and regularly publish certain categories of information without waiting for public requests. This obligation is outlined primarily under Articles 9 to 11, which specify the types of information that must be made available proactively, such as organizational structures, program activities, budget allocations, performance reports, procurement data, and decisions that affect the public interest.⁵¹

⁴⁸ Law No. 27 of 2022 on Personal Data Protection.

⁴⁹ Transparency International Indonesia. (2020). *Public Information Disclosure Assessment*.

⁵⁰ Law No. 14 of 2008 on Public Information Disclosure (Keterbukaan Informasi Publik).

⁵¹ Law No. 14 of 2008 on Public Information Disclosure (*Undang-Undang Keterbukaan Informasi Publik*), Articles 9–11.

However, implementation studies have shown that compliance with these provisions remains inconsistent. Despite the KIP Law's comprehensive regulatory design, many public authorities fail to routinely publish mandated information or update their public information pages as required under Article 7(2) and Article 9(3).⁵² This gap between legal obligation and administrative practice has been attributed to a combination of factors, including limited institutional capacity, inadequate data management systems, and weak enforcement mechanisms at both central and regional levels.⁵³

The table below summarizes the relevant sections of Law No. 14 of 2008 pertaining to proactive disclosure and highlights the corresponding institutional responsibilities.

Table 1. Provisions on Proactive Disclosure under Law No. 14 of 2008 on Public Information Disclosure

The following table summarizes the key provisions of Law No. 14 of 2008 on Public Information Disclosure (*Undang-Undang Keterbukaan Informasi Publik*, or KIP Law) that establish proactive disclosure obligations for public authorities. These provisions, set out in Part One (Articles 9–11), specify the types of information that must be periodically published, disclosed immediately, or made available at any time.

Part	Articles	What It Entails
One (1)	Article 9 — Information to be Supplied and Published Periodically	<p>Obligation: Public agencies are required to announce public information on a regular basis. Covered Information: Includes information about the agency's profile, activities, performance, financial reports, and other information specified in implementing regulations.</p> <p>Frequency: The disclosure of public information must occur at least semiannually (every six months).</p> <p>Accessibility: Information must be easily accessible to the public and presented in clear, simple language.</p> <p>Methods: Determined by the agency's Information Management and Documentation Officer (<i>Pejabat</i></p>

⁵² Transparency International Indonesia. (2020). *Public Information Disclosure Assessment*. Jakarta.

⁵³ Paramita, S. (2019). "Implementation Challenges of Indonesia's Freedom of Information Act." *Indonesian Journal of Governance Studies*, 7(2), 33–49.

		<p><i>Pengelola Informasi dan Dokumentasi, PPID).</i></p> <p>Regulation: Further detailed in the Technical Directives of the Information Commission (<i>Peraturan Komisi Informasi</i>).</p>
Two (2)	<p>Article 10 — Information to be Published Immediately</p>	<p>Obligation: Public agencies must immediately announce any information that could threaten public safety or order. Accessibility: The information should be easily accessible and communicated in simple, understandable language.</p>
Three (3)	<p>Article 11 — Information to be Available at Any Time</p>	<p>Obligation: Public agencies must provide public information at any time upon request, including: - A list of authorized public information - Decision results and supporting considerations - Policies and supporting documents - Project work plans and estimated budgets - Agreements with third parties - Records of public meetings - Standard operating procedures for public services - Reports on public information service performance Accessibility of Open Information: Public information must remain available through objection mechanisms or dispute resolution processes. Regulation: Implementation methods governed by the Technical Directives of the Information Commission.</p>

Source: Law No. 14 of 2008 on Public Information Disclosure (*Undang-Undang Keterbukaan Informasi Publik*), Part One, Articles 9–11.

4.2. Legal and Policy Frameworks on Openness and Information Access in Indonesia

4.2.1. Law No. 14 of 2008 on Public Information Disclosure (Right to Information Law)

Under this law, public bodies are mandated to provide, disclose, and issue authorized public information to requesters, ensuring that such information is accurate and not misleading.⁵⁴ They must establish information systems to facilitate efficient access and provide written considerations for policies, including political, security, and administrative aspects. Public bodies must also utilize both electronic and non-electronic means to fulfill these obligations.

The Right to Information (RTI) Law thus serves as the backbone of Indonesia's transparency regime, anchoring citizens' constitutional right to information (Article 28F of the 1945 Constitution). However, several complementary statutes also reinforce principles of openness and public access to information across various sectors.

4.2.2. Law No. 40 of 1999 on the Press

Freedom of the press in Indonesia not only safeguards the media's right to report and disseminate information but also recognizes the public's entitlement to seek, acquire, and share ideas and information.⁵⁵

Article 6 of the Press Law mandates the press to:

- Fulfill the public's right to know;
- Uphold democracy, the rule of law, and human rights;
- Respect diversity and pluralism; and
- Serve as a public watchdog over government and business.

The press thus plays a critical role in translating openness into public accountability, ensuring that citizens remain informed about public affairs and governance processes. Despite these provisions, however, studies indicate that proactive disclosure remains weak in practice.⁵⁶ This shortfall stems primarily from inefficient information management systems and limited institutional capacities within public agencies, which hinder consistent compliance with disclosure obligations.

4.2.3. Laws Supporting Whistleblower Protection and Anti-Corruption Efforts

⁵⁴ Law No. 14 of 2008 on Public Information Disclosure, Articles 9–11.

⁵⁵ Law No. 40 of 1999 on the Press, Article 6.

⁵⁶ Winastwan Gora Swajati, *Kajian Kebijakan dan Sistem Pengelolaan Data Penelitian Indonesia*, Bappenas, p. 19.

While Indonesia does not yet have a comprehensive whistleblower protection law, partial safeguards exist under the Law on Witness and Victim Protection (Law No. 13/2006, as amended by Law No. 31/2014).⁵⁷ This law authorizes the Witness and Victim Protection Agency (LPSK), reporting directly to the President, to protect individuals whose disclosures lead to criminal investigations.

Similarly, Law No. 31/1999 on the Eradication of Corruption Crimes, as amended by Law No. 20/2001, recognizes the importance of whistleblowers in uncovering corruption.⁵⁸ It mandates confidentiality, prohibits retaliation, and extends protection to whistleblowers categorized as witnesses in corruption cases. However, implementation gaps persist, particularly in ensuring anonymity and preventing institutional reprisals against those who expose wrongdoing.

4.2.4. Law No. 32 of 2009 on Environmental Protection and Management

Indonesia's commitment to transparency in environmental governance is reflected in the Environmental Protection and Management Act (EPMA). This law integrates transparency, participation, and accountability as core principles of environmental democracy. It mandates:

- Public access to environmental information;
- The obligation for polluters to disclose environmental risks; and
- The creation of environmental information systems to publish environmental status reports, vulnerability maps, and relevant datasets.⁵⁹

Through these mechanisms, the EPMA positions information disclosure as a precondition for community participation in environmental decision-making, an approach consistent with international environmental governance standards such as the Aarhus Convention and the Environmental Democracy Index (EDI).⁶⁰

4.2.5. International Commitments and Data Governance Implications

Indonesia's accession to the International Covenant on Civil and Political Rights (ICCPR) underscores the recognition of access to information as a human right, as

⁵⁷ Law No. 13 of 2006 on Witness and Victim Protection (as amended by Law No. 31/2014).

⁵⁸ Law No. 31 of 1999 on the Eradication of Corruption Crimes (as amended by Law No. 20/2001).

⁵⁹ Law No. 32 of 2009 on Environmental Protection and Management.

⁶⁰ United Nations Environment Programme (UNEP), *Environmental Democracy Index* (2019).

articulated in Article 19 of the Covenant.⁶¹ This international obligation strengthens Indonesia's legal foundation for data transparency, compelling the government to integrate human rights standards into data governance and information access frameworks.

Furthermore, Indonesia is a founding member of the Open Government Partnership (OGP) (2011), which has driven numerous reforms in public data accessibility and participatory governance.⁶² Through successive National Action Plans (NAPs), Indonesia has advanced initiatives such as the One Data Indonesia (Satu Data Indonesia) policy, promoting data standardization, interoperability, and proactive disclosure across ministries and agencies.⁶³

Indonesia also participates in several global transparency frameworks, including the ADB/OECD Anti-Corruption Initiative for Asia-Pacific, the OECD Busan Partnership for Effective Development Cooperation, the Extractive Industries Transparency Initiative (EITI), and the International Aid Transparency Initiative (IATI)⁶⁴. The practical implications of these engagements include:

- Strengthening cross-sector data standards;
- Expanding the volume and variety of publicly available datasets (especially on extractives and aid flows);
- Enhancing government accountability through peer review and international benchmarking; and
- Encouraging civil society participation in data-driven monitoring of governance outcomes.

4.2.6. State-Owned Enterprises (SOEs) and Information Disclosure

State-Owned Enterprises (SOEs) are bound by Law No. 19 of 2003 on State-Owned Enterprises and Government Regulation No. 45 of 2005 on SOE Establishment, Management, Supervision, and Dissolution, which require comprehensive disclosure of corporate information.⁶⁵ These include:

- Shareholding composition;
- Boards of Directors and Commissioners;
- Annual and financial reports;
- External audits and evaluations; and

⁶¹ United Nations, *International Covenant on Civil and Political Rights*, Article 19.

⁶² Open Government Indonesia, *National Action Plan 2023–2024* (Jakarta: Bappenas, 2022).

⁶³ Cabinet Secretariat of the Republic of Indonesia, *President Jokowi Issues Regulation on One Data Indonesia*, 27 June 2019.

⁶⁴ Asian Development Bank (ADB), *Data Management Policies and Strategies in Government* (2021).

⁶⁵ Government of Indonesia, *Law No. 19 of 2003 on State-Owned Enterprises*.

- Procurement mechanisms.

Such provisions align with the transparency principle under the RTI Law, ensuring that entities using public resources remain accountable to citizens.

4.2.7. Core Principles of Information Disclosure under Article 2 of Law No. 14 of 2008

The RTI Law establishes four guiding principles:

1. Openness: All public information is presumed open and accessible to every user.
2. Strict and Limited Exceptions: Exemptions are narrowly defined and must be justified through a consequence test balancing public and private interests.
3. Accessibility: Public information must be obtainable quickly, on time, at low cost, and through simple procedures.
4. Protection of Confidentiality: Information may be withheld only when disclosure would harm national security, economic resilience, personal privacy, or fair competition, as provided by law.⁶⁶

These principles reflect a balancing framework, upholding maximum disclosure while recognizing legitimate grounds for confidentiality.

4.2.8. Digital Transformation and Data-Based Policymaking

The National Open Government Action Plan (2018–2020) outlines Indonesia's data governance agenda, aiming to increase the value of data as a foundation for evidence-based policymaking.⁶⁷ This plan aligns with the Presidential Regulation No. 39 of 2019 on One Data Indonesia (Satu Data Indonesia) and Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems (SPBE), which set standards for data quality, metadata, interoperability, and master data management.⁶⁸

The One Data Initiative seeks to unify data across ministries and local governments, improving accuracy, accessibility, and consistency. It represents a major step toward data-driven governance, enhancing both administrative efficiency and public transparency.

⁶⁶ Law No. 14 of 2008 on Public Information Disclosure, Article 2.

⁶⁷ Open Government Partnership (OGP), *Indonesia Independent Reporting Mechanism (IRM) 2018–2020*.

⁶⁸ Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems.

5. Reactive Disclosure: The Right to Information (RTI) Framework

Indonesia's Right to Information (*Law No. 14 of 2008 on Public Information Disclosure*), establishes a framework for "reactive" disclosure, information made available upon request (*disclosure upon request*).⁶⁹ Under this mechanism, any individual or organization may request access to public information held by state institutions, provided that the information is not classified as exempt by law. Requesters are required to submit a clear statement of purpose to the relevant public agency, ensuring that the request falls within the purview of public interest.⁷⁰

The law obliges public authorities to respond within 10 working days, extendable by a further 7 days with written justification. Requests can be submitted in person, in writing, or electronically, though the law does not explicitly require agencies to adhere to the requester's preferred format⁷¹. Each public agency must designate an Information and Documentation Management Officer (*Pejabat Pengelola Informasi dan Dokumentasi – PPID*) responsible for processing requests and maintaining information systems. If the requested data are not within the agency's possession, the agency must inform the requester of where the information can be obtained; however, no mechanism for inter-agency transfer of requests is yet standardized (*Information Commission Regulation No. 1/2010*).⁷²

The RTI Law grants institutions limited authority to refuse disclosure, but such refusals are strictly regulated. Information may only be withheld for reasons explicitly enumerated in the law, including matters concerning law enforcement, intellectual property, defense and state security, national economic stability, natural wealth, diplomatic relations, or personal privacy.⁷³ With the exception of "natural wealth," all exemptions must undergo a harm test (*uji konsekuensi*), ensuring that disclosure would indeed result in substantive harm to the protected interest. In addition, the RTI framework imposes a public interest override, allowing information to be disclosed if the public benefit outweighs potential harm (*Article 2(4), Law No. 14/2008*).⁷⁴

Appeal procedures are embedded in the RTI framework. Requesters may file internal appeals to the supervising official of the relevant public body, and if unresolved, may escalate external administrative appeals to the Information

⁶⁹ Republic of Indonesia, *Law No. 14 of 2008 on Public Information Disclosure (UU KIP)*.

⁷⁰ *Ibid.*, Article 22–25.

⁷¹ *Ibid.*, Article 22(1).

⁷² Information Commission Regulation No. 1 of 2010 on Public Information Service Standards.

⁷³ Law No. 14 of 2008, Article 17.

⁷⁴ *Ibid.*, Article 2(4).

Commission (*Komisi Informasi*). The Commission functions as an independent oversight body, adjudicating disputes related to information access at the central, provincial, or regency/municipal levels. As a final recourse, litigants may seek judicial review through the courts⁷⁵.

While this framework provides a structured mechanism for reactive disclosure, challenges persist in practice. Studies by organizations such as the Centre for Law and Democracy (2021) and Transparency International Indonesia (2022) reveal that public authorities often fail to comply with procedural timelines, and response rates remain uneven across ministries and regional governments.⁷⁶ Moreover, low administrative capacity, fragmented information management systems, and limited digital literacy among PPIDs have hindered full implementation of the law.⁷⁷

5.1. Open Standards, Software Laws, and Administrative Practices

Indonesia's progress in implementing open data principles is closely tied to its broader e-government and administrative reform agenda. Despite legislative advances, implementation gaps remain evident. The United Nations E-Government Development Index (EGDI) ranked Indonesia 77th of 193 countries in 2022, lagging behind regional peers such as Malaysia, Thailand, and Singapore.⁷⁸ Similarly, the 2016 UN E-Government Readiness Index placed Indonesia at 109th, reflecting longstanding structural challenges.⁷⁹

A Presidential Executive Report (Kantor Staf Presiden, 2020) identified significant fragmentation in data governance practices across ministries and agencies. Many operate in silos, maintaining incompatible data systems without a unified framework for interoperability or data sharing.⁸⁰ This fragmentation undermines not only efficiency but also transparency, as inconsistent data standards impede the verification and publication of accurate information.

On the Open Government Data Index (OGDI), Indonesia scored 0.9014, placing it in the "Very High" category globally (Open Data Watch, 2022)⁸¹. However, this strong rating reflects formal commitments rather than consistent on-the-ground implementation.

⁷⁵ *Ibid.*, Articles 35–47.

⁷⁶ Transparency International Indonesia (2022). *Public Information Disclosure Implementation Report*.

⁷⁷ Centre for Law and Democracy (2021). *Global Right to Information Rating: Indonesia Profile*.

⁷⁸ United Nations (2022). *E-Government Development Index (EGDI)*.

⁷⁹ United Nations (2016). *E-Government Readiness Index Report*.

⁸⁰ Kantor Staf Presiden (2020). *Laporan Eksekutif: Evaluasi Tata Kelola Data Pemerintah*.

⁸¹ Open Data Watch (2022). *Open Government Data Index: Global Report*.

During the COVID-19 pandemic, priorities shifted toward crisis management, diverting attention from long-term data governance and protection issues. Although debates on the Personal Data Protection Law (Law No. 27 of 2022) have since advanced, earlier delays were attributed to competing policy priorities such as the controversial Job Creation Law (Omnibus Law) and pandemic response measure.⁸²

5.2. Data Protection in the Health Sector

Within the health sector, data protection frameworks have been primarily guided by Law No. 36 of 2009 on Health, which designates patients' medical records as confidential information.⁸³ While this provision affirms patients' right to control their personal data, the law lacks clear enforcement mechanisms, including administrative or criminal penalties for breaches. Moreover, no restitution or recovery framework exists for victims of data violations, revealing a significant regulatory gap in the protection of sensitive health information (Prasetyo & Hartono, *Journal of Law and Policy Studies*, 2020).⁸⁴

5.3. Policy Frameworks and Legal Foundations for the One Data Indonesia Initiative

The One Data Indonesia (Satu Data Indonesia / ODI) initiative, launched under Presidential Regulation No. 39 of 2019, represents Indonesia's key policy framework for ensuring accurate, standardized, and interoperable data across government institutions.⁸⁵ The initiative mandates that data produced by public bodies adhere to common data standards, include metadata, comply with interoperability rules, and utilize reference codes or master data to ensure consistency.⁸⁶

Implementation is led by BAPPENAS (Ministry of National Development Planning), with oversight by a Steering Council (SC) composed of ministers responsible for strategic sectors, and technical support provided by Central Data Trustees (CDT).⁸⁷ These entities are tasked with developing metadata structures, setting interoperability standards, and evaluating implementation progress. Further institutional arrangements were established through Ministerial Decree No.

⁸² Safitri, M. (2021). "Data Protection and Policy Priorities during the Pandemic." *Indonesian Journal of Law and Society*, 3(1).

⁸³ Republic of Indonesia, *Law No. 36 of 2009 on Health*, Article 57.

⁸⁴ Prasetyo, Y. & Hartono, D. (2020). "Health Data Protection in Indonesia: Legal Gaps and Future Prospects." *Journal of Law and Policy Studies*, 12(3).

⁸⁵ Republic of Indonesia, *Presidential Regulation No. 39 of 2019 on One Data Indonesia*.

⁸⁶ *Ibid.*, Articles 3–6.

⁸⁷ *Ibid.*, Article 10.

31/M.PPN/HK/04/2021, which created the Working Group for the Central-Level Indonesian One Data Forum.⁸⁸

The ODI initiative is also a key instrument for accelerating Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik / SPBE), which aims to enhance transparency, accountability, and inter-agency data connectivity.⁸⁹ Through this digital governance framework, the Indonesian government seeks to transform fragmented administrative data systems into a unified, interoperable data ecosystem that supports evidence-based policymaking.⁹⁰

Table 2. Key Legal Frameworks Regulating Access to Information and Data Governance in Indonesia

Law / Regulation (Official Title)	Specific Articles / Sections	Key Provisions and Stipulations
Law No. 14 of 2008 on Public Information Disclosure (Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik) ¹	Article 2	<ul style="list-style-type: none"> • Every item of public information is open and can be accessed by any user of public information. • Exemptions from disclosure are <i>strictly and narrowly defined</i>. - Applicants are entitled to obtain public information promptly, affordably, and through simple procedures. • Information can be withheld only if disclosure would cause harm outweighing the public interest in transparency. A <i>harm test</i> and <i>public interest test</i> are therefore embedded in the law.²

⁸⁸ Ministry of National Development Planning (BAPPENAS), *Ministerial Decree No. 31/M.PPN/HK/04/2021 on the Central-Level One Data Forum*.

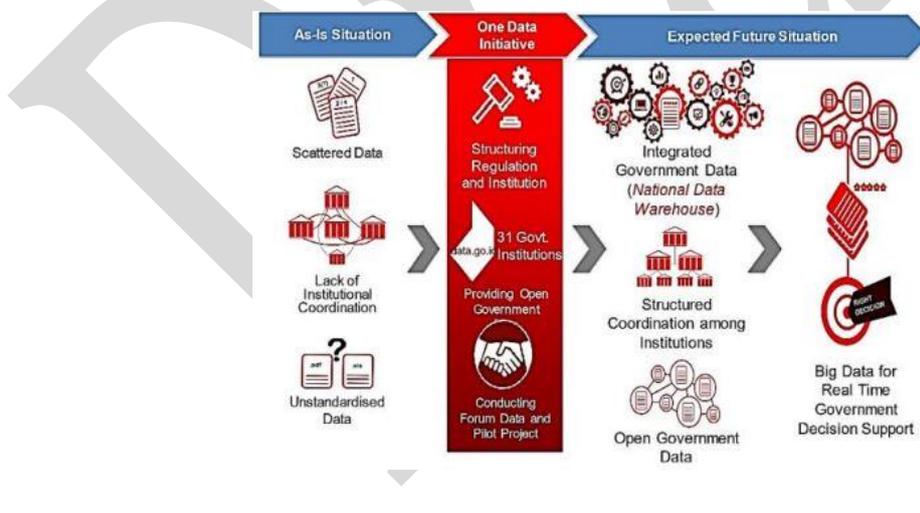
⁸⁹ Republic of Indonesia, *Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System (SPBE)*.

⁹⁰ BAPPENAS (2021). *One Data Indonesia Implementation Report*.

	Article 3	<ul style="list-style-type: none"> ● Establishes the objectives of the law, including: <ul style="list-style-type: none"> a. guaranteeing citizens' right to access information about policy plans, programs, and decision-making processes; b. encouraging public participation in policymaking; c. promoting transparency, accountability, and good governance in public bodies; d) improving information management and services to produce quality and accessible information. ● Explicitly mandates the government to facilitate public access to information as a means of strengthening participatory democracy.
<p>Presidential Regulation No. 39 of 2019 on One Data Indonesia (Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia)⁴</p>	Article 2	<ul style="list-style-type: none"> ● Regulates the governance of data produced by central and regional agencies to support national development planning, implementation, monitoring, and evaluation.- Establishes the objectives of <i>One Data Indonesia</i> to: <ul style="list-style-type: none"> a. provide a unified reference for data governance across government institutions; b. ensure that data is accurate, up-to-date, integrated, accountable, and easily accessible; c. improve coordination and data-sharing among agencies through standardized formats and interoperability principles. ● Provides a comprehensive regulatory framework defining institutional roles, responsibilities, and procedures for data collection, standardization, and dissemination.

<p>Ministerial Regulation of Communication and Informatics No. 1 of 2023 on Data Interoperability in the Implementation of Electronic-Based Government Systems and One Data Indonesia (Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2023 tentang Interoperabilitas Data dalam Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik dan Satu Data Indonesia)⁶</p>	<p>Article 2</p>	<ul style="list-style-type: none"> • Defines the two types of interoperability implementation: a) <i>National-level interoperability (LID Nasional)</i>; and b) <i>Interoperability implemented by central and regional agencies</i> within the framework of Electronic-Based Government Systems (SPBE) and <i>One Data Indonesia</i>. • Serves as the implementing regulation of Article 9(3) of Presidential Regulation No. 39/2019. • Aims to develop standardized mechanisms for interoperability and data sharing between government entities, supporting integrated e-government practices.
--	------------------	--

Picture I: Current condition and future expected situation with ODI⁹¹



5.4. Standards and Governance under the One Data Indonesia Framework

⁹¹ Nugroho, Y. (2017). *After Data Synchronising and Sharing - What Do We Learn? Lesson from Satu Data*. Jakarta: Kantor Staf Presiden RI.

Under Presidential Regulation No. 39 of 2019 on One Data Indonesia, the initiative is to be implemented based on a set of clearly defined data governance principles. These include:

1. Data produced by government agencies (*data producers*) must comply with data standards;
2. Data must be accompanied by metadata to ensure traceability and contextual understanding;
3. All datasets must adhere to interoperability rules, allowing data exchange and integration across government systems; and
4. All data must use reference codes and/or master data to maintain consistency and comparability across institutions.⁹²

To operationalize these principles, the government established the One Data Indonesia Portal, an open-access digital platform that serves as the national hub for public sector data. The portal facilitates information exchange and publication through the use of information and communication technology (ICT) infrastructure, thereby improving accessibility and transparency.⁹³

Institutionally, the Central One Data Indonesia (ODI) governance framework is organized around four key entities:

- the Steering Council, which provides policy direction;
- the Central Data Trustees, responsible for technical coordination and implementation;
- the Central Data Supervisory Institutions, ensuring compliance with standards and interoperability requirements; and
- the Central Data Producers, which generate and maintain datasets within their respective mandates.⁹⁴

At both central and regional levels, data dissemination is facilitated through the One Data Indonesia website (satudata.go.id), which functions as a unified gateway for accessing verified datasets. As of August 2023, the initiative had integrated approximately 214,240 datasets shared across 53 ministries and central government agencies, 27 provincial governments, and 213 regional governments throughout Indonesia.⁹⁵ This level of integration reflects significant

⁹² Presidential Regulation No. 39 of 2019 on One Data Indonesia (*Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia*), Article 3.

⁹³ *Ibid.*, Article 9; see also One Data Indonesia Portal (*Portal Satu Data Indonesia*), available at <https://satudata.go.id>

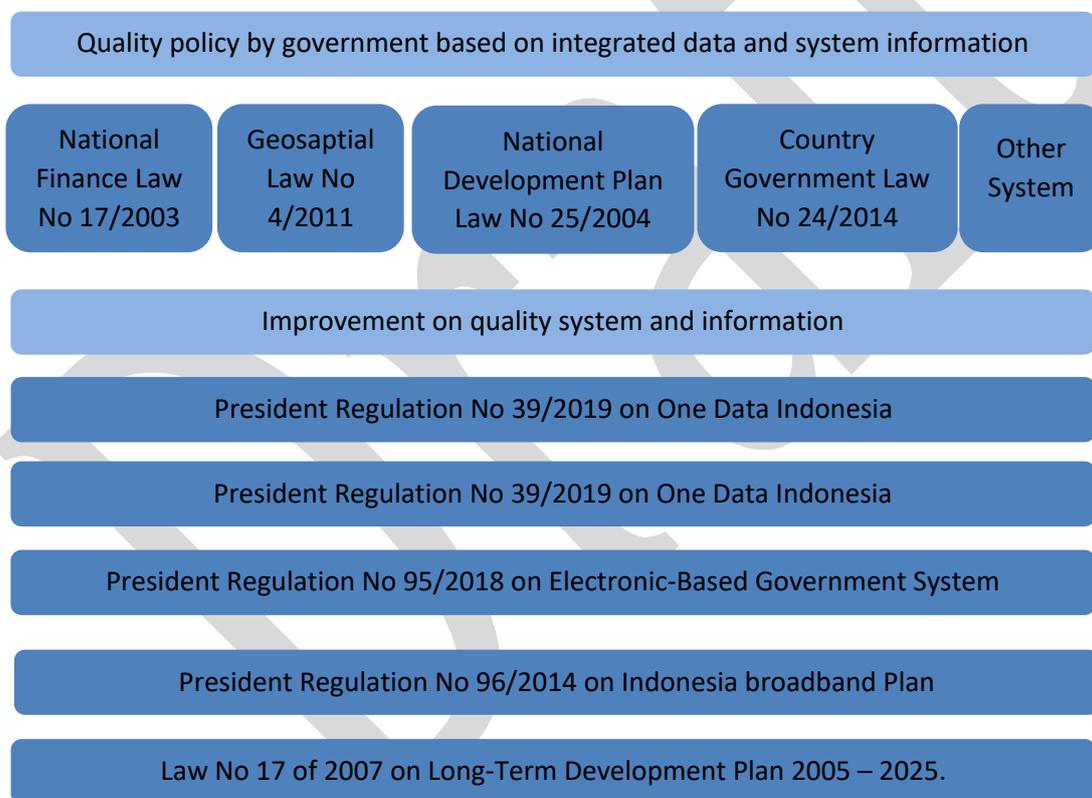
⁹⁴ *Ibid.*, Articles 4–6, which specify institutional roles and coordination mechanisms.

⁹⁵ Ministry of National Development Planning/Bappenas, *One Data Indonesia Progress Report*, August 2023.

progress in inter-agency coordination and the institutionalization of data-sharing mechanisms under the One Data framework.

The One Data Indonesia Initiative also serves as an acceleration instrument for the implementation of Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems (EBGS). The EBGS framework aims to enhance public service delivery through the development of effective, transparent, accountable, and trustworthy digital governance. The linkage between these two regulations underscores Indonesia’s strategic effort to promote data-driven policymaking and digital transformation within the public sector by strengthening data connectivity and interoperability among government institutions.⁹⁶

Picture 2: Transformation Plan by Government⁹⁷



6. Decreasing Openness: Security and Legal Restrictions on Access

6.1. Security

⁹⁶ Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems (*Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*), Articles 2–5.

⁹⁷ Presidential Regulation No. 39 of 2019 on One Data Indonesia

While the Government of Indonesia continues to promote transparency through the Right to Information (RTI) Law (Law No. 14 of 2008), it also maintains a complex legal framework that restricts access to certain categories of information. These restrictions are justified on grounds of national security, privacy, law enforcement, and economic stability, reflecting the state's effort to balance openness with protection of sensitive data.⁹⁸

Under the RTI Law, public bodies are required to proactively disclose information; however, Article 17 of the Law enumerates ten categories of information exempt from public access. These include:

1. disclosures that could hinder law enforcement processes or endanger informants;
2. information affecting the protection of intellectual property and fair business competition;
3. information on defense and security strategies;
4. disclosures related to Indonesia's natural wealth;
5. information that could threaten national economic stability or diplomatic relations;
6. personal data or medical records; and
7. confidential communications between public institutions.⁹⁹

The law also mandates that exemptions must be applied restrictively, subject to both a *harm test* and a *public interest override*. This means information can only be withheld if disclosure would clearly cause harm, and even then, it must be released if doing so serves a greater public interest¹⁰⁰. Despite these safeguards, implementation often leans toward over-classification, reflecting a cautious government stance on openness.

Additionally, Article 65 of the Personal Data Protection Law (Law No. 27 of 2022) provides exceptions to personal data rights when processing data for national defense, law enforcement, financial supervision, or statistical and scientific research.¹⁰¹ These broad exemptions allow government bodies significant discretion in determining what information is withheld, contributing to what civil society observers describe as a *shrinking space for public data access*.

⁹⁸ Law No. 14 of 2008 on Public Information Disclosure (Right to Information Act).

⁹⁹ Ibid., Article 17.

¹⁰⁰ Ibid., Article 19 (Harm Test) and Article 20 (Public Interest Override).

¹⁰¹ Law No. 27 of 2022 on Personal Data Protection, Article 65.

The RTI Law also allows internal and external appeals for denied requests. Internally, complaints can be submitted to the Information and Documentation Management Officer (PPID) supervisor, while externally, disputes can be brought to the Information Commission (Komisi Informasi) at national, provincial, or district levels¹⁰². However, these mechanisms often face delays and limited enforcement power, limiting their effectiveness in ensuring government openness.

6.2. The Role of the National Data Center (NDC)

The establishment of the National Data Center (NDC) under Presidential Regulation No. 132 of 2022 on Electronic-Based Government Systems (SPBE) represents the government's ambition to centralize and secure public data infrastructure.¹⁰³ According to Article 27, the NDC functions as a shared facility for storing, processing, and recovering government data, interconnecting central and local agencies under the coordination of the Ministry of Communication and Informatics (Kominfo).

While the NDC aims to enhance efficiency and data integrity, its centralized control over data storage and access introduces new limitations to openness. Unlike decentralized agency systems, where some datasets were directly accessible through public portals, the NDC consolidates data management within a closed government environment, potentially restricting public and inter-agency access unless formally authorized.¹⁰⁴

Thus, the NDC exemplifies a shift toward data sovereignty: ensuring data is stored domestically and under state supervision. This reduces risks from cross-border data breaches but simultaneously narrows data accessibility for civil society, journalists, and researchers seeking real-time government datasets.

6.3. Digital Integration and Data Access Controls

The government's digital transformation agenda, guided by Presidential Regulation No. 82 of 2023 on Priority SPBE Applications, aims to accelerate interoperability across government systems. The regulation mandates that "Priority SPBE Applications", those serving at least 200,000 users, must

¹⁰² Law No. 14 of 2008, Chapter VII, Articles 35–47.

¹⁰³ Presidential Regulation No. 132 of 2022 on Electronic-Based Government Systems (SPBE).

¹⁰⁴ Ministry of Communication and Informatics (Kominfo). (2023). *National Data Center Implementation Guidelines*.

integrate through shared government infrastructure to ensure security and efficiency.¹⁰⁵

Although interoperability is conceptually linked to greater openness and accessibility, in practice, this policy emphasizes integration within government systems rather than open access to the public. The intent is to streamline internal data flow between ministries while tightening external access controls, reflecting a broader pattern where “digital efficiency” coexists with reduced public transparency.

In this context, “SPBE” (Sistem Pemerintahan Berbasis Elektronik) refers to Electronic-Based Government Systems, encompassing applications and digital services managed by government agencies.¹⁰⁶ These systems operate under a security-first model where data sharing is inward-facing, between government entities, rather than outward-facing to the public. This aligns with Indonesia’s evolving cybersecurity doctrine, prioritizing data protection and national sovereignty over unrestricted openness.

6.4. Intelligence and Security Oversight

The State Intelligence Law (Law No. 17 of 2011) further codifies limits on information disclosure in the name of national security. The law grants extensive authority to the State Intelligence Agency (Badan Intelijen Negara – BIN) to collect, analyze, and safeguard state secrets¹⁰⁷. However, it has been criticized for vague definitions of “threats to national security”, particularly under Article 6(3), which could enable broad and arbitrary interpretation of security risks.

Articles 26, 44, and 45 of the Law prescribe prohibitions and penalties to prevent misuse, yet lack procedural safeguards to ensure proportionality and oversight in intelligence operations. As a result, the line between legitimate secrecy and overreach remains blurred, raising concerns among civil society organizations about the potential chilling effect on freedom of expression and public accountability.¹⁰⁸

The 2011 Law also intersects with the RTI framework, as intelligence-related data are automatically classified as non-disclosable, with criminal

¹⁰⁵ Presidential Regulation No. 82 of 2023 on Priority SPBE Applications.

¹⁰⁶ Kominfo. (2023). *Digital Transformation Roadmap 2021–2024*.

¹⁰⁷ Law No. 17 of 2011 on State Intelligence.

¹⁰⁸ Setiyono, B. & Ariyanto, B. (2022). *Secrecy and Transparency in Indonesia’s National Security Governance*. *Journal of Indonesian Legal Studies*, 7(1).

penalties, including imprisonment and fines, or unauthorized disclosures. This overlap underscores how national security frameworks override transparency norms, limiting public access to information even on matters of broad societal relevance.

6.5. Sectoral Data Protection Frameworks

Indonesia's legal ecosystem governing personal and institutional data remains fragmented across multiple sectoral regulations, reinforcing the trend toward controlled disclosure:

1. Demographic Data Protection: *Law No. 23 of 2006*, as amended by *Law No. 24 of 2013 on Demographic Administration*, regulates the protection of personal data collected for demographic purposes (e.g., ID cards, population registries).¹⁰⁹
2. Health Sector Data Protection: *Ministry of Health Regulation No. 24 of 2022 on Medical Records* governs the confidentiality, retention, and deletion of patient data.¹¹⁰
3. Banking and Financial Data Protection: *Bank Indonesia Regulation No. 3 of 2023* updates earlier regulations to strengthen financial data privacy and cybersecurity requirements.¹¹¹

While these frameworks enhance privacy safeguards, they also reinforce restrictions on access to public-interest information, as agencies interpret confidentiality clauses broadly to avoid potential violations.

Indonesia's regulatory environment reveals a dual dynamic: while it upholds constitutional guarantees of the right to information, it simultaneously expands legal instruments that justify secrecy, from cybersecurity and personal data protection to intelligence operations and centralized data governance. This reflects a global shift toward "data sovereignty", but in the Indonesian case, it also manifests as decreasing openness, where the pursuit of security and efficiency inadvertently contracts public access to information essential for democratic accountability.

7. Privacy and Data Protection in Indonesia

¹⁰⁹ Law No. 23 of 2006 as amended by Law No. 24 of 2013 on Demographic Administration.

¹¹⁰ Ministry of Health Regulation No. 24 of 2022 on Medical Records.

¹¹¹ Bank Indonesia Regulation No. 3 of 2023 on Data and Information Protection in the Banking Sector.

7.1. Constitutional and Human Rights Foundations

Indonesia's Constitution, the *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*, explicitly recognizes privacy as a fundamental human right. Article 28G(1) affirms that "every person deserves protection for themselves, their family, their honor, their dignity, and their belongings, and they also deserve a sense of security and protection from any threats that push them to do or not do something." This article establishes the constitutional basis for privacy and personal data protection as an extension of human dignity and security.¹¹²

Furthermore, Law No. 39 of 1999 on Human Rights reinforces the right to privacy, particularly emphasizing the confidentiality of communication and correspondence through electronic means.¹¹³ This creates the normative groundwork for recognizing data privacy as part of human rights protection, even before sectoral regulations on data governance were introduced.

As Indonesia's internet penetration has grown, reaching over 210 million users in 2023, concerns over personal data misuse have intensified. The policy discourse has thus evolved beyond mere user protection toward a broader focus on the governance of data collection, processing, storage, and utilization across both public and private sectors.¹¹⁴

7.2. Personal Data Protection Law (Law No. 27 of 2022)

The Personal Data Protection (PDP) Law, enacted on October 17, 2022, represents Indonesia's first comprehensive data protection regime, harmonizing previously fragmented regulations.¹¹⁵ The law applies to all entities, public or private, engaged in personal data processing, whether operating domestically or abroad, provided that their processing activities impact individuals within Indonesia.

The PDP Law establishes key principles governing data processing: lawfulness, fairness, transparency, purpose limitation, data minimization,

¹¹² *The 1945 Constitution of the Republic of Indonesia (UUD 1945)*, Article 28G(1).

¹¹³ *Law No. 39 of 1999 on Human Rights*, Articles 32–34.

¹¹⁴ Ministry of Communication and Informatics (Kominfo). (2023). *Indonesia Digital Report 2023*.

¹¹⁵ *Law No. 27 of 2022 on Personal Data Protection (PDP Law)*.

accuracy, storage limitation, integrity and confidentiality, and accountability. Controllers and processors are granted a two-year transition period (until October 2024) to comply, pending the issuance of 11 implementing regulations mandated under the law.¹¹⁶

7.3. Institutional Framework and Oversight

To enforce the PDP Law, Indonesia is in the process of forming a dedicated Data Protection Authority (DPA), referred to as the Indonesian DPA, which will be responsible for policymaking, supervision, enforcement, and dispute resolution.¹¹⁷ Until the DPA is formally established, the Ministry of Communication and Informatics (MOCI/Kominfo) continues to act as the interim supervisory authority, overseeing compliance within the Electronic Information and Technology (EIT) sector.

Under Government Regulation No. 71 of 2019 (GR 71/2019) and MOCI Regulation No. 20 of 2016, MOCI has the authority to:

- Oversee cross-border data transfers involving electronic system operators (ESOs);
- Receive and act upon data breach notifications;
- Supervise personal data protection in electronic systems; and
- Impose administrative sanctions for non-compliance.¹¹⁸

In sector-specific areas, supervision is decentralized:

- The Financial Services Authority (OJK) and Bank Indonesia (BI) regulate personal data within financial services, banking, and payment systems;
- The Ministry of Health (MoH) oversees medical data through its regulations on health information systems and patient confidentiality.¹¹⁹

7.4. Legal Bases for Processing and Key Exceptions

¹¹⁶ Kominfo (2023). *PDP Law Implementation Roadmap*.

¹¹⁷ *Ibid.*, Articles 55–58.

¹¹⁸ *Government Regulation No. 71 of 2019 on Electronic Systems and Transactions (GR 71/2019)*; *MOCI Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems*.

¹¹⁹ *OJK Regulation No. 6/POJK.07/2022*; *Ministry of Health Regulation No. 24 of 2022 on Medical Records*.

Under the PDP Law, personal data processing must rely on one or more legal bases, which include:

1. Consent of the data subject;
2. Fulfillment of contractual obligations;
3. Compliance with legal obligations of the controller;
4. Protection of vital interests of the data subject;
5. Public interest or execution of duties by public authorities; and
6. Legitimate interests of the controller, provided such interests do not override the data subject's rights.¹²⁰

This framework mirrors global standards such as the EU GDPR, allowing flexibility beyond mere consent. However, in practice, Indonesian controllers still rely heavily on consent-based mechanisms, often through standard consent forms or digital “click-wrap” agreements.

The PDP Law also provides exceptions to the exercise of data subject rights and restrictions on processing, particularly when processing is conducted for:

- National defense and security;
- Law enforcement purposes;
- Public administration;
- Financial supervision or systemic stability; or
- Statistics and scientific research.¹²¹

These exceptions illustrate the balancing act between privacy protection and state or institutional imperatives, mirroring the cautious approach seen in Indonesia's RTI and security legislation.

7.5. Rights of Data Subjects

The PDP Law provides comprehensive rights to individuals whose data is processed. These include:¹²²

1. Right to Obtain Information – to know the identity, legal basis, and purpose of processing;

¹²⁰ PDP Law, Article 20.

¹²¹ PDP Law, Article 65.

¹²² PDP Law, Chapter V (Articles 5–15).

2. Right to Complete, Update, or Rectify Data – to ensure accuracy and relevance;
3. Right to Access Data or Copies – to view or obtain copies of their personal data;
4. Right to Erasure and Processing Termination – to request deletion or termination of processing;
5. Right to Withdraw Consent – at any time, without affecting the lawfulness of prior processing;
6. Right to Object to Automated Decision-Making – including profiling that affects individuals significantly;
7. Right to Restrict Processing – to limit the processing for specific purposes;
8. Right to Data Portability – to obtain and reuse their data across different controllers;
9. Right to File Complaints – before the DPA;
10. Right to Legal Remedies – including compensation claims for damages from violations.

These rights collectively align Indonesia with global privacy frameworks, enhancing user empowerment while maintaining procedural flexibility for government and private controllers.

7.6. Sectoral Data Protection Regulations

a. Healthcare Sector

The Health Law of 2023 (enacted July 11, 2023) introduces comprehensive rules governing personal health information, medical records, and health technology data.

- Article 4 establishes the confidentiality of personal health data, with exceptions for law enforcement, epidemic management, education and research, public safety, insurance, and patient consent.
- Articles 306–309 require healthcare professionals to maintain medical records, guarantee their integrity, and uphold confidentiality. Medical records belong to healthcare facilities but patients retain access rights to their content.
- Article 359 expands on biomedical and digital health technologies, such as genomics and precision medicine,

mandating explicit consent for specimen collection, storage, and use, except when data is anonymized or used for scientific or legal purposes.¹²³

While these provisions strengthen health data governance, implementation challenges persist, particularly around the interoperability of health systems, data sharing between facilities, and clarity on anonymization standards.

b. Financial and Consumer Protection

The Financial Sector Development and Strengthening Law (P2SK Law) also addresses consumer data protection, including provisions for cross-border data transfer.¹²⁴ It permits data transfer outside Indonesia's jurisdiction, provided it complies with domestic data protection principles.

Complementing this, Bank Indonesia Regulation No. 3 of 2023 mandates that financial institutions must obtain explicit consumer consent before transferring personal data, whether domestically or internationally.¹²⁵ These provisions aim to balance innovation and fintech growth with stringent privacy guarantees.

Indonesia's data protection regime reflects a hybrid approach, it aspires to meet global privacy standards while accommodating the government's priorities of national security, administrative control, and economic governance. The PDP Law's broad exceptions, sectoral overlaps, and pending establishment of the DPA highlight an ongoing transition from fragmented regulation toward a unified yet state-centric privacy governance model. As implementation proceeds, the key challenge lies in ensuring that privacy protections are substantive and enforceable, not merely formal. The coming years, particularly after full enforcement of the PDP Law, will determine whether Indonesia's data protection framework advances genuine digital rights protection or primarily administrative control.

¹²³ *Health Law No. 17 of 2023*, Articles 4, 306–309, 359.

¹²⁴ *Financial Sector Development and Strengthening Law (P2SK Law, 2023)*.

¹²⁵ Bank Indonesia Regulation No. 3 of 2023 on Data and Information Protection in the Banking Sector.

8. Deep Dives

8.1. Leveraging Co-Creation as an Equilibrium Mechanism for Involving Non-Governmental Actors in Data Governance

The governance of public data represents a complex equilibrium between transparency, accountability, and the protection of privacy. While the public increasingly demands access to information that reflects how public policy is designed, implemented, and evaluated, governments must develop a structured mechanism that both safeguards sensitive data and promotes inclusive participation. This balancing act, between openness and control, requires innovative governance approaches that institutionalize the involvement of non-governmental actors such as civil society organizations, academia, private sector innovators, and community groups.¹²⁶

Co-creation emerges as a viable equilibrium mechanism for this purpose. It involves the joint design, implementation, and monitoring of public policies or services between government institutions and non-state actors. By embedding co-creation principles in data governance, governments can expand their outreach and ensure that policy frameworks respond to societal needs with legitimacy and trust. In an era characterized by digital acceleration and heightened concerns over surveillance and privacy, trust in public institutions is no longer solely determined by their authority but by their demonstrated social value, through ethical, secure, and transparent data practices.¹²⁷

Meaningful public participation across the stages of policymaking, especially in program formulation, data collection, and evaluation, has been shown to significantly improve policy quality and service delivery outcomes.¹²⁸ When citizens are invited to participate in defining problems and validating solutions, the resulting policies are not only more effective but also more credible. Over time, this participatory process enhances institutional performance and builds a cycle of trust between government and citizens. Institutionalizing co-creation through frameworks that codify data governance, integrating data from multiple sectors into a coherent system, provides an

¹²⁶ OECD (2020). *The Path to Open Government: How to Strengthen Co-creation and Collaboration in Public Policy*.

¹²⁷ World Bank (2021). *Trust, Data, and Governance in the Digital Age*.

¹²⁸ Fung, A. (2015). *Putting the Public Back into Governance: The Challenges of Citizen Participation and Co-production*.

additional layer of credibility to decision-making and legitimizes the outcomes of policy processes.¹²⁹

Indonesia's **Open Government Indonesia (OGI)** initiative exemplifies this co-creation model, particularly in the context of open data and digital innovation. OGI's framework for co-creation delivers four primary benefits to data governance:

1. **Information Disclosure Empowering Citizens**— Co-creation strengthens mechanisms of information disclosure, empowering citizens not only to access data but to utilize it in improving public services and holding institutions accountable.¹³⁰
2. **Public Involvement in Service Assessment** – It fosters participatory evaluation, allowing citizens to directly contribute to assessing service performance and identifying areas for reform.
3. **Public Participation in Designing and Ensuring Service Quality** – Citizens, when engaged in co-designing public services, bring diverse perspectives that enhance inclusivity and responsiveness in service delivery.¹³¹
4. **Inclusion Mechanism for Marginalized Groups** – Co-creation also acts as an instrument of social inclusion, facilitating the participation of marginalized groups such as women, persons with disabilities, and the elderly, whose voices are often underrepresented in formal governance processes.¹³²

Nonetheless, challenges remain in Indonesia's implementation of co-creation, particularly in ensuring that points three and four above are not merely rhetorical but embedded in institutional practices. The active engagement of excluded or vulnerable communities requires continuous policy refinement, inclusive design principles, and equitable access to data platforms.

At the national level, the engagement of civil society within the framework of the Open Government Partnership (OGP) has significantly improved Indonesia's transparency practices. The Open Budget Index (OBI) survey conducted by the International Budget Partnership (IBP) in 2017 ranked

¹²⁹ UNDESA (2019). *E-Government Survey 2019: Digital Government in the Decade of Action for Sustainable Development*.

¹³⁰ Open Government Indonesia (2022). *OGI National Action Plan 2021–2023*.

¹³¹ OECD (2019). *Innovative Citizen Participation and New Democratic Institutions: Catching the Deliberative Wave*.

¹³² UN Women (2022). *Gender and Data Governance in the Digital Age*.

Indonesia with a score of 64, one position below the Philippines in the region.¹³³ The OBI measures transparency by assessing the quantity and timeliness of budget information accessible to the public through the Open Budget Survey (OBS). This progress indicates that participatory governance and co-creation mechanisms contribute positively to improving public access to government data.

However, despite these advancements, Indonesia still faces persistent challenges in enhancing transparency and data visibility across critical sectors. These include inconsistencies in data sharing, uneven implementation of privacy protection frameworks, and the limited institutional capacity for managing open data at the subnational level.¹³⁴ Notably, sectoral initiatives in finance and health have demonstrated both progress and fragmentation. For instance, while the **Financial Services Authority (OJK)** has established regulations protecting consumer data in financial services,¹³⁵ The health sector continues to grapple with interoperability and privacy issues, as evidenced by the implementation challenges of the **SATUSEHAT** platform.¹³⁶

Addressing these challenges requires a comprehensive framework for co-creation that institutionalizes collaboration between government, civil society, academia, and the private sector. Such a framework should prioritize:

- **Institutional alignment** – ensuring that data-sharing standards are harmonized across agencies;
- **Capacity building** – developing digital literacy among both officials and citizens;
- **Regulatory coherence** – establishing consistent data protection and ethical use standards across sectors; and
- **Inclusive participation** – embedding marginalized groups within data governance processes, not as beneficiaries but as co-creators.

In this context, co-creation should not be perceived merely as a participatory ideal but as a **governance instrument**, an equilibrium mechanism that reconciles the state's regulatory authority with society's participatory rights. By leveraging co-creation, Indonesia can move toward a model of **collaborative data governance**, where transparency, accountability, and inclusivity reinforce

¹³³ International Budget Partnership (2017). *Open Budget Survey: Indonesia Country Report*.

¹³⁴ Kominfo (2023). *Evaluation of Open Data and Digital Governance Implementation in Indonesia*.

¹³⁵ OJK Circular No. 14/SEOJK.07/2014 on Confidentiality and Security of Consumer Data.

¹³⁶ Ministry of Health Regulation No. 24/2022 on Electronic Medical Records.

one another, forming the foundation for sustainable trust and democratic resilience in the digital era.¹³⁷

8.2 Increasing vs Decreasing: The Latest Developments in Indonesian Policy and Regulations on Data Governance

The governance of data in Indonesia presents a dynamic duality: on one hand, substantial efforts have been made to increase openness, interoperability, and public access to governmental data; on the other hand, significant measures of restriction, fragmentation and institutional inertia continually challenge those gains. This section charts the trajectory of Indonesia's policy and regulatory developments, highlighting the "increasing" trends towards openness and the "decreasing" or constraining trends that complicate the realization of a fully transparent data ecosystem.

8.2.1 Increasing Access: Surveys, Portals, and Institutional Commitments

One of the foundational pillars of Indonesia's data governance improvements lies in the continuous operation of large-scale national surveys by BPS – Statistics Indonesia. These include:

- Sakernas (the National Labour Force Survey), conducted twice annually across all provinces;
- Susenas (the National Socioeconomic Survey), covering households to generate indicators of health, education, consumption, and welfare; and
- Podes (Village Potential Survey), capturing socio-economic characteristics at the village and sub-district level.

For example, in March 2022, Susenas covered approximately 345,000 households across regular census blocks. The 2018 Podes survey documented 83,931 administrative units at the village level, including 75,436 villages and 8,444 urban villages.¹³⁸ Such comprehensive data collection

¹³⁷ World Economic Forum (2023). *Data for Common Purpose Initiative (DCPI): Advancing Data Collaboration in the Public Sector*.

¹³⁸ Jurnal Spektrum Komunikasi (Maulana Arief & Amalia Nurul Muthmainnah). "Data Journalist: One Data Indonesia (SDI) Weak of Data" (2023).

underscores Indonesia's commitment to evidence-based planning and public data generation.

In parallel, Indonesia's ranking in global transparency metrics has improved. According to the International Budget Partnership (IBP) Open Budget Survey (OBS), Indonesia's budget transparency improved: by 2021 Indonesia ranked 17th out of 120 countries, climbing from 23rd out of 115 in 2017. [Antara News](#) This upward movement underscores that the state is increasingly recognising the importance of publicly available fiscal data and accountability mechanisms.

Furthermore, the One Data Indonesia initiative, formalised by Presidential Regulation No. 39 of 2019, aims to unify and integrate government data across levels and agencies, promoting interoperability, data standardisation, and open-data access protocols.¹³⁹ Studies have shown that the One Data implementation can enhance data credibility, availability and public usage, particularly when local government agencies engage in data sharing and standard alignment.¹⁴⁰

Collectively, these developments illustrate the "increasing" trend, through expanded data collection, improved transparency rankings, institutional frameworks for open data, and enhanced aspirations for data-driven governance.

8.2.2 Decreasing or Constraining Access: Fragmentation, Access Costs, and Institutional Barriers

Despite the gains, substantial constraints remain. Implementation of One Data Indonesia, for instance, continues to face multiple structural obstacles: a large number of data guardians (ministries, regions, agencies) with varying standards; mismatches between data production and policy needs; insufficient standardisation of metadata; a lack of effective data sharing and interoperable platforms; and limited human resources to manage and govern data assets.¹⁴¹ This fragmentation contributes to reduced public accessibility even though data may technically exist.

¹³⁹ Ramadhan et al., "One Data Indonesia: A Retrospective Analysis of Data Interoperability in Declaring Regional Planning and Development," *KnE Social Sciences*, Vol. 10 (16) (2023).

¹⁴⁰ Islami, Maulia Jayantina. "Implementasi Satu Data Indonesia: Tantangan dan Critical Success Factors (CSFs)," *Jurnal Komunika*, Vol. 10 No. 1 (2023).

¹⁴¹ "5 Issues in Satu Data Implementation," *Jiwa Muda Indonesia*, June 17 2022.

An illustrative example: while BPS data collection is robust, the previously open access to detailed datasets (such as full Susenas microdata) has become more restricted and subject to licensing or high cost due to commercial use risks, such as cases where a tobacco company exploited the data for marketing. This shift from “open on request” to restricted access signals a decreasing openness in practice, albeit often driven by legitimate data-use concerns.¹⁴²

Moreover, access to data often remains contingent on capacity, institutional readiness, or financial cost. Without unified policy enforcement and adequate resourcing, many public institutions struggle to publish data proactively, maintain updated datasets, or provide user-friendly access interfaces. These limitations result in the gap between policy aspiration and operational reality.

8.2.3 Trade-Offs and Interplay: Openness vs Control, Innovation vs Standardisation

The interplay between increasing and decreasing trends reveals key trade-offs in Indonesia’s data governance ecosystem. Three major interrelated trade-offs stand out:

- **Data Quality vs. Data Quantity:** While more data is being collected, many datasets lack accurate, complete, or up-to-date attributes. Poor data quality reduces utility and trust, undermining the “space of openness” despite the existence of large volumes.
- **Centralisation vs. Decentralisation:** Initiatives such as One Data Indonesia and the push for unified national portals favour centralisation for interoperability and oversight. Yet, Indonesia’s decentralised administrative geography, with 34 provinces and hundreds of districts/cities, demands flexibility and local responsiveness. The tension between uniformity and local autonomy thus constrains open access in practice.
- **Regulatory Compliance vs. Innovation:** Imposing data standards, metadata requirements, secure sharing protocols, and strict licensing may safeguard governance and control, but may also inhibit agility, experimentation, and rapid innovation, particularly in sectors like fintech

¹⁴² Utama, Difa Pramudya & Lina Miftahul Jannah. “Tantangan Implementasi Satu Data Penerbangan dan Antariksa,” *Media Bina Ilmiah*, Vol. 16 No. 12 (2024).

or

data

journalism.

Each of these trade-offs epitomises the dual dynamics of “increasing” and “decreasing” within the same system: while the legislative frameworks and infrastructure aim for openness, the operational, institutional and contextual realities can undermine the practical availability and accessibility of data.

8.2.4 Sectoral Highlights: Finance, Health and Open Data Sustainability

In the financial sector, the regulatory framework emphasises confidentiality and security of consumer data, e.g., the Otoritas Jasa Keuangan (OJK) introduced rules specifying sensitive data points (such as mother’s maiden name, date of birth, address) for protection. These obligations reinforce public trust but can also limit the extent to which aggregated or anonymised data is released for public innovation.¹⁴³

In the health sector, digital infrastructures such as the SatuSehat platform aim to consolidate patient data, integrate healthcare facility systems, and support policy monitoring. While these initiatives signal increased data capability and transparency, they also bring concerns around privacy, third-party data processing, and unequal implementation across regions. Inconsistent deployment and unclear governance structures highlight the persistent gap between “data existence” and “data accessibility.”

These sectoral snapshots demonstrate how openness is being built, but also concurrently constrained, by regulatory, technical and organisational layers.

8.2.5 Looking Forward: Bridging the Gap Between Aspiration and Practice

For Indonesia to realise the full potential of its data governance ambitions, the following conditions must be addressed:

1. Institutional Coordination and Governance Maturity: The proliferation of data trustees, platforms, and standards must be governed through coherent oversight and accountability mechanisms. As identified in One

¹⁴³ “Kemenkeu sebut keterbukaan penganggaran Indonesia terus meningkat,” ANTARA News, Feb 15 2023.

Data implementation studies, alignment across central and regional actors is essential.¹⁴⁴

2. Capacity Building and Human Resources: Without sufficiently trained personnel, sophisticated infrastructure and consistent standards will remain under-utilised. Investing in digital literacy, data stewardship roles, and local government readiness is critical.
3. Open Data Usability and Proactive Disclosure: Beyond data publication, proactive disclosure matters. User-friendly portals, metadata standards, open licensing, and cost-free access will determine whether data is truly open in practice.
4. Balancing Protection with Access: Legal frameworks must continue to guard privacy, national security and economic interests, but also ensure that such protections do not become default barriers to public access or innovation.
5. Sustainable Finance and Infrastructure: Open data ecosystems require ongoing funding, infrastructure upkeep, platform interoperability and data refresh cycles. Without sustainable investment, openness may stagnate or regress.

By addressing these enablers, Indonesia can shift the data governance narrative from “aspiration with constraints” to “action with impact”, thereby enhancing transparency, trust, innovation and public service outcomes.

¹⁴⁴ OJK Circular No. 14/SEOJK.07/2014 on Confidentiality and Security of Consumer Data.