JLPGD
Journal of Law, Policy and Global Development

# Journal of Law, Policy and Global Development

**ISSN(Online): 3109-3965**
**Vol 1 no 1 (2025): June 2025**
*https://journal.as-salafiyah.id/index.php/jlpgd/index*
*Email: editorjlpgd@gmail.com*

# Digital Governance And The Right To Privacy: A Comparative Analysis Of AI Regulation In Southeast Asia And The European Union

**[1]Muh Habibulloh**
*[1]Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung, Indonesia*
*[1]habibulloh040689@gmail.com*

*Correspodence Email: habibulloh040689@gmail.com*

***Abstract:*** *This study investigates the evolving regulatory landscape of artificial intelligence (AI) and personal data protection through a comparative legal analysis between Southeast Asia (ASEAN) and the European Union (EU). As AI technologies increasingly permeate public governance, economic systems, and everyday decision-making, they introduce complex legal and ethical challenges related to algorithmic accountability, privacy rights, and data security. The EU, exemplified by the General Data Protection Regulation (GDPR) and the proposed Artificial Intelligence Act, has developed a rights-based, precautionary regulatory model rooted in fundamental freedoms and democratic oversight. In contrast, ASEAN member states display considerable diversity in legal frameworks, enforcement capacities, and normative approaches—often prioritizing innovation, digital competitiveness, and pragmatic governance over stringent privacy safeguards. Employing a doctrinal and comparative methodology, this study analyzes statutes, institutional structures, and regional policy initiatives such as the ASEAN Framework on Digital Data Governance. The findings reveal significant regulatory asymmetries but also emerging areas of convergence. The study concludes by advocating for enhanced regional cooperation, capacity-building, and the adoption of adaptive, risk-based legal frameworks that align technological development with human rights standards. These insights contribute to the broader global discourse on ethical digital governance and the achievement of the UN Sustainable Development Goals (SDGs), particularly Goal 16 on peace, justice, and strong institutions.*
***Keywords****: Artificial Intelligence Regulation, Data Privacy, GDPR, Human Rights, Comparative Law.*

## INTRODUCTION

The rise of artificial intelligence (AI) is transforming the global landscape of governance, public administration, and socio-economic systems. Across both developed and developing countries, AI applications are being integrated into state services, justice systems, health care, education, and national security, offering unprecedented opportunities for efficiency, prediction, and innovation. However, as AI becomes more embedded in decision-making structures, the risks

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

to fundamental human rights particularly the right to privacy are increasingly apparent. AI systems operate by processing vast quantities of personal and behavioral data, often with minimal human oversight. This reliance on data-intensive processes raises significant concerns regarding consent, data security, transparency, bias, and accountability (Floridi et al., 2018; Gstrein, 2021).

One of the central challenges facing policymakers is how to regulate AI in a manner that enables innovation while safeguarding human dignity and individual rights. A key domain within this challenge is the regulation of data privacy, which has become a cornerstone of digital governance. Without robust data protection laws, individuals are vulnerable to surveillance, discrimination, and loss of autonomy. The regulatory responses to these issues have varied significantly across regions. The European Union (EU), with its strong tradition of rights-based governance, has taken a leading role in establishing comprehensive legal frameworks aimed at regulating AI and protecting personal data. Its General Data Protection Regulation (GDPR), enacted in 2018, is considered one of the most advanced data protection laws globally and has influenced numerous jurisdictions beyond Europe (Voigt & Von dem Bussche, 2017).

The GDPR provides individuals with enforceable rights such as access to personal data, the right to be forgotten, and the right to data portability. It also introduces principles of fairness, purpose limitation, and accountability for data controllers. In 2021, the EU further reinforced its commitment to responsible AI by proposing the Artificial Intelligence Act (AIA), which classifies AI systems based on the level of risk they pose and imposes corresponding regulatory obligations (European Commission, 2021). This layered, risk-based approach reflects the EU's broader strategy to ensure that AI serves society while protecting its most vulnerable members.

In contrast, the regulatory landscape in Southeast Asia is diverse and uneven. ASEAN countries exhibit a spectrum of legal maturity and institutional capacity in the area of AI and data governance. Singapore and Malaysia, for example, have implemented national data protection laws—the Personal Data Protection Act (PDPA) in Singapore and the Personal Data Protection Act 2010 in Malaysia—that provide a baseline framework for regulating personal information (Chander, 2021). These laws emphasize data use transparency and consumer protection but often

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

prioritize economic competitiveness and technological advancement over human rights guarantees.

Other ASEAN countries, such as Indonesia, Thailand, and the Philippines, are in various stages of legislative reform, seeking to align more closely with international standards. Indonesia's enactment of the Personal Data Protection Law in 2022 marks a significant step forward, although implementation and enforcement mechanisms remain under development (Mahardhika, 2022). Thailand's PDPA, which came into effect in 2022, shares many features with the GDPR, yet the lack of an independent oversight body limits its enforcement strength (Raab & Szekely, 2017). The Philippines, Vietnam, and Cambodia continue to work on foundational frameworks, with uneven progress and limited regional coherence.

Southeast Asia's regulatory inconsistencies are also shaped by deeper political and institutional factors. In some countries, privacy is not enshrined as a constitutional right, and state surveillance practices are widespread. The absence of strong judicial or administrative oversight further limits the effectiveness of privacy regulation. In addition, digital policy discourse in the region often emphasizes economic growth and innovation as central objectives, sometimes at the expense of privacy rights (Tapsell, 2020; Ong, 2019). Regional strategies, such as the ASEAN Digital Masterplan 2025, highlight digital transformation, e-commerce, and AI adoption but offer little guidance on rights-based governance models (ASEAN, 2021).

Despite these disparities, there are signs of convergence. Many ASEAN countries are increasingly influenced by international legal norms, particularly those embodied in the GDPR. Cross-border cooperation in data governance is also emerging through ASEAN platforms. However, achieving regulatory harmonization remains a challenge due to divergent political priorities, legal traditions, and levels of institutional development (Kuner et al., 2017). The lack of a supranational body akin to the European Commission or Court of Justice of the European Union limits ASEAN's ability to enforce uniform standards.

This article conducts a comparative analysis of AI regulation and the right to privacy in the EU and selected ASEAN countries, offering insights into how legal systems conceptualize and

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

operationalize digital governance. While the EU offers a structured, rights-based, and enforceable model of AI regulation, ASEAN countries offer pragmatic and adaptive approaches shaped by economic and developmental needs. Understanding these regional approaches is critical, not only for legal harmonization but also for fostering inclusive, ethical, and sustainable AI ecosystems worldwide.

A comparative perspective provides value by identifying both transferable principles and context-specific limitations. It can serve as a foundation for building interoperable frameworks that enable cross-border data flows while ensuring adequate rights protection. Furthermore, such a perspective is aligned with the goals of the United Nations 2030 Agenda for Sustainable Development, particularly Goal 16, which calls for strong institutions, access to justice, and protection of fundamental freedoms (UNDP, 2020). In an era of increasing reliance on AI, aligning digital innovation with democratic values is not a luxury it is a necessity.

## METHOD

This study adopts a qualitative, comparative legal research design, using the doctrinal method as its foundational analytical approach. The research focuses on interpreting and evaluating legal texts and institutional practices to understand how different jurisdictions regulate artificial intelligence (AI) and protect the right to privacy. By employing doctrinal analysis, the study systematically reviews statutory instruments, policy documents, case law, and academic commentaries from both the European Union (EU) and the Association of Southeast Asian Nations (ASEAN).

The selection of sources includes primary legal materials, such as the General Data Protection Regulation (GDPR), the proposed EU Artificial Intelligence Act (2021), and key rulings from the Court of Justice of the European Union (CJEU). From the ASEAN region, national data protection laws from Singapore, Malaysia, Indonesia, and Thailand were examined, alongside regional policy frameworks like the ASEAN Digital Masterplan 2025. Supplementary data were also gathered from publications of international organizations such as the Organisation for

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

Economic Co-operation and Development (OECD), the United Nations (UN), and the Asia-Pacific Economic Cooperation (APEC), as well as peer-reviewed academic literature on AI governance and digital law.

The analytical framework centers on comparative legal analysis, emphasizing both legal convergence and divergence between the EU and ASEAN systems. Thematic focus is placed on three critical areas: the underlying legal definitions and regulatory principles, the design and capacity of enforcement mechanisms, and the extent to which rights-based safeguards are integrated into AI regulation. By comparing jurisdictions with regulatory leadership (EU) and regulatory diversity (ASEAN), this methodology enables a nuanced exploration of global digital governance trends, offering valuable insights into the balance between innovation, legality, and human rights protection.

## RESULT AND DISCUSSION

### Regulatory Frameworks: A Rights-Based vs. Innovation-Oriented Approach

The regulatory approaches to artificial intelligence (AI) and data governance in the European Union (EU) and Southeast Asian nations (ASEAN) are shaped by distinct legal cultures, political institutions, and developmental priorities. The EU framework is grounded in a rights-based normative structure, emphasizing human dignity, transparency, fairness, and accountability, while many ASEAN member states prioritize innovation, digital competitiveness, and flexible regulation to support economic growth.

At the core of the EU's AI governance model are two pivotal legal instruments: the General Data Protection Regulation (GDPR) and the proposed Artificial Intelligence Act (AIA). The GDPR, which came into force in 2018, is widely regarded as a global benchmark for personal data protection. It sets a high bar by mandating informed consent, data minimization, purpose limitation, and strong enforcement through independent supervisory authorities (Voigt & Von dem Bussche, 2017). In 2021, the European Commission introduced the AIA, which classifies AI applications by risk levels—unacceptable, high, limited, and minimal—and establishes

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

corresponding obligations. High-risk systems, such as those used in biometric identification or critical infrastructure, must undergo mandatory impact assessments, ensure human oversight, maintain data quality standards, and be auditable. Violations of these provisions could lead to fines of up to €30 million or 6% of global annual turnover (European Commission, 2021).

In contrast, ASEAN countries exhibit a heterogeneous and evolving regulatory landscape, often described as fragmented and development-driven. Rather than adopting a unified rights-based approach, most ASEAN jurisdictions emphasize economic pragmatism and regulatory flexibility. Table 1 below summarizes the comparative status of AI and data protection regulations in selected ASEAN countries.

| Country | Data Protection Law | AI Regulatory Status | Enforcement Strength | GDPR Alignment |
|---|---|---|---|---|
| **Singapore** | PDPA (revised 2020) | AI Ethics Framework (voluntary) | Moderate | Partial |
| **Malaysia** | PDPA 2010 | No formal AI law | Moderate | Limited |
| **Thailand** | PDPA (effective 2022) | Draft AI policy | Weak | Partial |
| **Indonesia** | PDP Law (enacted 2022) | Under development | Weak | Emerging |
| **Vietnam** | Draft data protection decree | No AI-specific law | Weak | Low |
| **Philippines** | Data Privacy Act (2012) | No AI-specific regulation | Moderate | Low |

***Table 1.*** *AI and Data Protection Frameworks in Selected ASEAN Countries (as of 2024).* Sources: ASEAN Secretariat (2023); National ICT Ministries; UNCTAD (2021); Mahardhika (2022)

Singapore presents a unique case in the region. Its Personal Data Protection Act (PDPA), revised in 2020, provides robust data governance mechanisms but leans toward a "light-touch" co-regulatory model. The government has also developed a Model AI Governance Framework, which promotes voluntary adherence to principles such as explainability, fairness, and human-centricity (IMDA, 2020). However, these remain non-binding guidelines without statutory enforcement mechanisms.

Malaysia and Thailand have implemented formal data protection laws, but enforcement remains inconsistent, largely due to institutional constraints and political inertia (Raab & Szekely, 2017). Thailand's PDPA, modeled in part on the GDPR, still lacks an operational Data Protection

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

Authority as of early 2024. Indonesia's Personal Data Protection Law, enacted in 2022, is a landmark achievement, yet it remains in an early implementation phase. Key issues include the absence of detailed implementing regulations and capacity-building within the designated oversight body (Mahardhika, 2022).

Meanwhile, countries like Vietnam and the Philippines are still grappling with foundational regulatory issues. Vietnam's data protection decree remains in draft form, and the Philippines, despite having an established Data Privacy Act, has yet to address AI-specific challenges. Across the region, AI deployment is accelerating faster than legal and institutional developments, creating gaps in accountability and public trust (Chander, 2021).

The EU's rights-based framework provides a clear contrast, with binding legal obligations, strong enforcement through Data Protection Authorities, and a harmonized legal environment across member states. ASEAN's more innovation-oriented approach reflects regional priorities such as digital transformation, economic competitiveness, and attracting foreign investment, but often lacks legal clarity and uniformity.

Ultimately, these differing frameworks reflect broader governance philosophies. The EU treats data and AI governance as matters of fundamental rights and democratic accountability, whereas ASEAN tends to view them as technical and economic issues, best handled through soft regulation and policy experimentation. While both models have advantages, the lack of enforceable safeguards in much of Southeast Asia raises concerns about individual rights, ethical AI use, and long-term societal trust in digital systems.

**The Right to Privacy in AI Governance**

The integration of artificial intelligence (AI) into both public and private spheres has necessitated a reexamination of how the right to privacy is protected in digital governance systems. In the European Union (EU), the right to privacy is firmly embedded in the Charter of Fundamental Rights of the European Union, specifically under Article 7 (Respect for private and family life) and Article 8 (Protection of personal data). This constitutional grounding elevates privacy beyond

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

a mere statutory guarantee, making it a binding normative principle that must guide the design, deployment, and oversight of AI systems.

This legal philosophy is clearly reflected in the General Data Protection Regulation (GDPR), which sets comprehensive obligations for data controllers and robust rights for individuals. Central to the GDPR are the principles of data minimization, purpose limitation, consent, and transparency (Voigt & Von dem Bussche, 2017). It grants data subjects enforceable rights—such as the right to access, right to rectification, right to erasure ("right to be forgotten"), and right to object to automated decision-making—that are directly relevant to mitigating harms from AI systems. These safeguards ensure that individuals retain a degree of agency and oversight even in highly automated environments (Wagner & Janssen, 2021).

In contrast, ASEAN countries tend to approach privacy from a statutory rather than constitutional perspective, leading to fragmented protections that vary widely by country and sector. Most ASEAN member states do not explicitly enshrine the right to privacy in their constitutions, which limits its enforceability and weakens its normative weight. Instead, privacy rights are often embedded in sector-specific legislation or administrative codes, which are inconsistently applied and weakly enforced (Mahardhika, 2022).

| Region/Country | Constitutional Protection of Privacy | Enforceable Data Subject Rights | Restrictions on Automated Decision-Making | Oversight Body with Enforcement Powers |
|---|---|---|---|---|
| **European Union** | Yes (Charter of Fundamental Rights) | Yes (GDPR Art. 12–22) | Yes (Art. 22 GDPR) | Yes (DPAs in each member state) |
| **Singapore** | No | Yes (PDPA) | Partial (voluntary ethics) | Yes (PDPC) |
| **Malaysia** | No | Limited | No explicit provision | Partial (PDP Commission) |
| **Indonesia** | No | Emerging (UU PDP 2022) | Under development | Planned but not operational |
| **Thailand** | No | Yes (PDPA 2022) | Weak enforcement | In development |
| **Vietnam** | No | Draft only | No | No |

***Table 2.*** *Privacy Protection in AI Governance: EU vs. Selected ASEAN Countries (2024). Sources: ASEAN Legal Instruments (2023), European Data Protection Board (2023), Mahardhika (2022)*

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

The discrepancy in legal foundations is mirrored in practice. In Singapore, for example, the Personal Data Protection Act (PDPA) provides a regulatory framework for privacy but emphasizes business trust and compliance rather than individual empowerment. The Personal Data Protection Commission (PDPC) offers voluntary guidelines for AI ethics, yet these are non-binding, and do not confer enforceable rights regarding automated profiling or algorithmic decisions (IMDA, 2020). Similarly, Malaysia's PDPA, enacted in 2010, lacks provisions that directly address algorithmic harm or the rights of individuals affected by automated decisions.

Indonesia's Personal Data Protection Law (UU PDP), passed in 2022, aligns partially with GDPR principles, introducing the right to access and correct personal data. However, its practical impact remains limited due to a lack of institutional infrastructure and clear enforcement mechanisms. Thailand's PDPA, which came into effect in 2022, includes data subject rights but has been criticized for slow implementation and vague protections related to AI-specific use cases (Raab & Szekely, 2017).

In some ASEAN jurisdictions, national security concerns further erode privacy protections. For instance, state surveillance programs and centralized biometric databases are often exempted from data protection laws, creating regulatory blind spots. These exceptions are rarely subject to judicial review, and oversight bodies—where they exist—lack independence or the mandate to investigate government practices (Tapsell, 2020). Such environments pose significant risks when AI is used in law enforcement, immigration control, or public service delivery.

The EU model stands in sharp contrast. The GDPR's Article 22 prohibits solely automated decisions that produce legal or similarly significant effects unless specific safeguards are in place, such as explicit consent or suitable human oversight. This provision is critical in the context of AI-driven profiling, where decisions can affect employment, credit scoring, and social services eligibility. The European Data Protection Board (EDPB) has issued extensive guidance on the application of these rights, reinforcing the role of human judgment in AI governance (EDPB, 2022).

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

While ASEAN nations have made commendable progress in developing national privacy laws, the lack of constitutional recognition, combined with inconsistent enforcement, limits their ability to ensure meaningful protection in the age of AI. Bridging this regulatory gap will require not only legal reform but also institutional strengthening, regional cooperation, and a normative shift toward viewing privacy as a fundamental and enforceable right rather than a policy goal.

**Enforcement and Institutional Capacities**

The effectiveness of AI governance and data privacy protection depends not only on the quality of legislation but also on the strength of enforcement mechanisms and institutional capacities. In the European Union (EU), enforcement is supported by a well-established, multi-level regulatory architecture composed of independent Data Protection Authorities (DPAs) in each member state and the European Data Protection Board (EDPB), which coordinates cross-border oversight and ensures consistency in the application of the General Data Protection Regulation (GDPR). These institutions are empowered with investigatory, corrective, and advisory powers, including the ability to impose administrative fines of up to €20 million or 4% of global annual turnover, whichever is higher (Voigt & Von dem Bussche, 2017).

National DPAs across the EU have demonstrated increasing enforcement activity since the implementation of the GDPR. For instance, in 2023 alone, data protection authorities in France, Germany, and Ireland imposed fines exceeding €2 billion collectively, mostly targeting large tech companies for non-compliance with consent and data transparency requirements (EDPB, 2023). The EDPB also plays a strategic role by issuing guidelines on emerging technologies, including the use of AI in biometric identification and algorithmic decision-making.

In contrast, the enforcement landscape in ASEAN is more fragmented and inconsistent. While most countries in the region have enacted data protection laws, the institutional infrastructure for implementation and oversight remains underdeveloped. This disparity results from differences in regulatory maturity, political will, financial resources, and technical expertise.

JLPGD
Journal of Law, Policy and Global Development

# Journal of Law, Policy and Global Development

**ISSN(Online): 3109-3965**
**Vol 1 no 1 (2025): June 2025**
*https://journal.as-salafiyah.id/index.php/jlpgd/index*
*Email: editorjlpgd@gmail.com*

| Country/Region | National DPA Established | Independent Authority | Enforcement Powers | Budget Transparency | Cross-Border Cooperation |
|---|---|---|---|---|---|
| **European Union** | Yes (all 27 members) | Yes | Strong | Yes | High (via EDPB) |
| **Singapore** | Yes (PDPC) | Partial | Moderate | Yes | Limited |
| **Malaysia** | Yes (PDP Commission) | Partial | Limited | No | Limited |
| **Indonesia** | Planned (under UU PDP) | No (under formation) | Weak (early stage) | No | Low |
| **Thailand** | Yes (Office of PDPC) | No (Gov't reporting) | Weak | No | Low |
| **Vietnam** | No | No | None | No | None |

***Table 3.*** *Institutional Capacities for Data Protection Enforcement in the EU and Selected ASEAN Countries (2024). Sources: ASEAN ICT Reports (2023), EDPB Annual Report (2023), UNCTAD Digital Economy Report (2021)*

Singapore stands out in the region for its relatively advanced enforcement capacity. The Personal Data Protection Commission (PDPC) is an operational agency with a clear mandate, and it has issued multiple enforcement decisions against both domestic and foreign companies for breaches of the Personal Data Protection Act (PDPA). However, critics argue that the PDPC lacks full independence, given its status as a statutory board under the Ministry of Communications and Information (IMDA, 2020). Moreover, Singapore's emphasis on promoting innovation sometimes limits the scope and severity of enforcement action (Chander, 2021).

Malaysia's Personal Data Protection Department (PDPD) operates under the Ministry of Communications and Digital, with limited independence. Its enforcement activities are often constrained by budget limitations, lack of human resources, and the absence of a clear procedural framework for dealing with AI-related complaints. As of 2023, no major enforcement actions against AI misuse have been reported, highlighting the gap between legislation and enforcement (Raab & Szekely, 2017).

Indonesia is in the early stages of institutionalizing its data protection regime. While the Personal Data Protection Law (UU PDP) mandates the creation of an independent supervisory authority, the body had yet to be operationalized by mid-2024. Interim oversight responsibilities

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

are held by the Ministry of Communication and Information Technology (Kominfo), raising concerns about conflicts of interest and regulatory capture (Mahardhika, 2022).

Thailand's Office of the Personal Data Protection Committee, established under its Personal Data Protection Act (PDPA), remains structurally dependent on the government. Although the law provides for administrative penalties, the institutional body lacks the necessary resources, legal clarity, and enforcement personnel to carry out its mandate effectively (UNCTAD, 2021).

A key challenge across ASEAN is the absence of a regional enforcement mechanism comparable to the EDPB in the EU. Without a coordinated institutional framework, cross-border data enforcement remains weak, especially in areas involving multinational AI service providers or cloud-based platforms. Although the ASEAN Framework on Digital Data Governance promotes cooperation, it lacks binding provisions or standardized protocols for joint investigations and redress mechanisms (ASEAN, 2021).

The EU experience demonstrates the importance of independent oversight, adequate resourcing, and regional coordination in sustaining effective enforcement. The success of GDPR enforcement owes much to the institutional authority and capacity of national DPAs and their ability to collaborate through the EDPB. By contrast, ASEAN's lack of institutional depth and harmonization presents a risk that even well-drafted privacy laws will remain toothless in practice.

To strengthen enforcement, ASEAN countries must invest in institution-building, provide adequate funding, and guarantee the independence of oversight bodies. Moreover, the region could benefit from creating an ASEAN-level coordinating body for data protection—modeled, perhaps, on the EDPB—to facilitate dialogue, training, and cross-border case handling. Only through such institutional enhancement can AI governance in Southeast Asia ensure real accountability and protection of privacy rights.

**Regulatory Convergence and Policy Recommendations**

Despite the evident regulatory divergence between the European Union (EU) and the Association of Southeast Asian Nations (ASEAN) in the field of artificial intelligence (AI) and data governance, a gradual process of regulatory convergence is beginning to emerge. The

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

convergence is most visible in the formulation of shared digital governance principles, the establishment of national data protection laws, and efforts to develop regionally coherent frameworks.

Initiatives such as the ASEAN Framework on Digital Data Governance (2018) and the ASEAN Digital Masterplan 2025 signal a collective interest in developing interoperable standards for data protection, cross-border data flows, and algorithmic transparency (ASEAN, 2021). These documents endorse principles such as data sovereignty, security, innovation enablement, and inclusive digital transformation. While these frameworks are largely non-binding, they represent a foundational step toward long-term regulatory harmonization and signal policy alignment with global norms, particularly those outlined by the OECD, APEC, and the European Commission.

The EU, through instruments like the GDPR and the proposed Artificial Intelligence Act, has demonstrated a robust model of risk-based regulation rooted in fundamental rights and democratic accountability. ASEAN member states, though at different stages of regulatory maturity, have increasingly shown interest in adapting select EU principles, such as impact assessments, data subject rights, and algorithmic fairness, albeit with flexibility for local economic and legal contexts.

| Area of Regulation | EU (Status) | ASEAN (Emerging Practices) | Convergence Level |
|---|---|---|---|
| **Risk-Based AI Regulation** | High (EU AI Act) | Low to Moderate (Singapore, Thailand drafts) | Moderate |
| **Data Protection Laws** | Full Harmonization (GDPR) | Partial (6 ASEAN states with PDP laws) | Moderate |
| **Independent Oversight Bodies** | Fully operational | Partial or developing | Low |
| **Cross-Border Data Flow Mechanisms** | Coordinated via EDPB | Initial regional strategy (AFDDG) | Low to Moderate |
| **Public Consultation in AI Policy** | Mandatory (EU Commission) | Voluntary or ad hoc | Low |

***Table 4.*** *Indicators of Regulatory Convergence: EU vs. ASEAN (2024). Sources: European Commission (2021), ASEAN Secretariat (2021), IMDA (2020), UNCTAD (2022)*

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

To accelerate regulatory convergence and ensure responsible AI governance, this study proposes a multi-dimensional policy framework tailored to regional capabilities and governance structures. The following four recommendations are essential to advancing both digital innovation and rights protection in ASEAN and similar regions:

1. Strengthen Independent Oversight Bodies

A critical enabler of enforceable governance is the existence of well-resourced, independent supervisory authorities. These bodies must be legally empowered to conduct investigations, impose sanctions, and provide policy guidance. ASEAN nations should expedite the institutionalization of data protection agencies and ensure their autonomy from executive interference (Raab & Szekely, 2017).

2. Promote Public Participation and Stakeholder Engagement

Transparent and inclusive AI policymaking processes enhance democratic legitimacy and increase public trust. While the EU mandates public consultation and impact assessments, most ASEAN countries rely on closed-door decision-making. Governments in Southeast Asia are encouraged to institutionalize multi-stakeholder forums, particularly involving civil society, academia, and private sector actors (Floridi et al., 2018).

3. Enhance Regional Cooperation on Cross-Border Data Governance

AI systems often operate transnationally, making cross-border data flow a core regulatory concern. ASEAN should move beyond voluntary frameworks and work toward legally binding regional agreements on data transfer, modeled on standard contractual clauses used in the EU. A dedicated ASEAN Data Protection Council could help coordinate responses to cross-border enforcement and emerging AI threats (Chander, 2021).

4. Adopt Risk-Based Regulatory Models with Local Adaptation

ASEAN countries should consider adapting the EU's risk-based classification system outlined in the AI Act. However, this should be done with sensitivity to local priorities and capacities. For example, lower-income states may prioritize economic inclusion and infrastructure over complex regulatory mechanisms. A tiered regulatory strategy, beginning with high-risk

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

sectors such as facial recognition or predictive policing, would allow for targeted capacity-building (Wagner & Janssen, 2021).

These recommendations underscore the need for a contextual and phased approach to regulatory development one that allows ASEAN nations to balance innovation incentives with human rights safeguards. While full harmonization with the EU may be aspirational in the short term, incremental legal alignment, policy dialogue, and regional standard-setting remain feasible and beneficial pathways.

## CONCLUSION

The regulation of artificial intelligence (AI) and the protection of personal data have emerged as central pillars of digital governance in the 21st century. As AI technologies increasingly influence public administration, commercial transactions, and societal behavior, the demand for robust, accountable, and rights-oriented regulatory frameworks becomes ever more urgent. This study has undertaken a comparative analysis of the European Union (EU) and selected ASEAN countries to examine how different regions conceptualize and implement legal protections for privacy and algorithmic accountability. The findings reveal that the EU has established a comprehensive and precautionary approach, grounded in the Charter of Fundamental Rights and operationalized through instruments such as the General Data Protection Regulation (GDPR) and the proposed Artificial Intelligence Act. These legal mechanisms emphasize human dignity, transparency, and risk mitigation, ensuring that technological innovation does not come at the expense of individual rights and societal trust.

In contrast ASEAN member states follow a more diverse and development-oriented trajectory. While countries like Singapore and Thailand have advanced data protection regimes, others are still in the process of institutionalizing basic safeguards. Enforcement capacity, regulatory coherence, and public participation remain uneven across the region. Nonetheless, there are promising signs of convergence, particularly through initiatives such as the ASEAN Framework on Digital Data Governance. Achieving a more inclusive, ethical, and globally aligned

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

digital order will require sustained inter-regional dialogue, capacity-building in less developed jurisdictions, and the establishment of shared global principles. As AI continues to reshape governance, law, and society, integrating legal safeguards with technological design will be essential not only to protect the right to privacy but also to foster responsible, human-centered innovation on a global scale.

## REFERENCE

ASEAN. (2021). *ASEAN Digital Masterplan 2025*. ASEAN Secretariat. https://asean.org

ASEAN. (2021). *Framework on Digital Data Governance*. ASEAN Secretariat. https://asean.org

ASEAN. (2023). *ASEAN Digital Economy Framework Agreement Working Draft*. ASEAN Secretariat. https://asean.org

Chander, A. (2021). Data nationalism and the rise of digital sovereignty. *Emory Law Journal*, 70(4), 1281–1312.

EDPB. (2023). *Annual Report 2022*. European Data Protection Board. https://edpb.europa.eu

European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu

European Data Protection Board. (2022). *Guidelines 05/2021 on the interaction between the GDPR and AI systems*. https://edpb.europa.eu

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Gstrein, O. J. (2021). The rights to privacy and data protection in times of crisis: A legal analysis of COVID-19 tracking apps. *Computer Law & Security Review*, 41, 105529.

IMDA. (2020). *Model AI Governance Framework (2nd Edition)*. Infocomm Media Development Authority. https://www.imda.gov.sg

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2017). The GDPR: Understanding the EU's data protection framework. *International Data Privacy Law*, 7(1), 1–13.

Journal of Law, Policy and Global Development
ISSN(Online): 3109-3965
Vol 1 no 1 (2025): June 2025
https://journal.as-salafiyah.id/index.php/jlpgd/index
Email: editorjlpgd@gmail.com

Mahardhika, A. (2022). Regulatory dilemmas in Southeast Asia's digital transformation. *Journal of Southeast Asian Legal Studies*, 5(2), 117–138.

OECD. (2022). *OECD Framework for the Classification of AI Systems*. https://www.oecd.org

Ong, J. C. (2019). Data justice and the politics of digital infrastructures in Southeast Asia. *Media, Culture & Society*, 41(7), 994–1002.

Raab, C. D., & Szekely, I. (2017). Data protection authorities and information technology. *Computer Law & Security Review*, 33(4), 421–431.

Sartor, G. (2020). The Artificial Intelligence Act: Regulating AI through risk classification. *European Journal of Risk Regulation*, 11(4), 683–697.

Tapsell, R. (2020). Southeast Asia's digital authoritarianism. *Democratization*, 27(3), 495–512.

Tjong Tjin Tai, E. (2020). Legal aspects of artificial intelligence. *Computer Law & Security Review*, 36, 105389. https://doi.org/10.1016/j.clsr.2020.105389

UNCTAD. (2021). *Digital Economy Report 2021: Cross-border data flows and development*. United Nations Conference on Trade and Development. https://unctad.org

UNDP. (2020). *Human Development Report 2020: The next frontier—Human development and the Anthropocene*. United Nations Development Programme. https://hdr.undp.org

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Wagner, B., & Janssen, C. (2021). AI and fundamental rights: Balancing innovation and safeguards. *Human Rights Law Review*, 21(2), 245–267.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.