Table 1: Data Governance Landscape in Major ASEAN Countries (This table reflects the most recent legal and regulatory developments in data protection, cross-border data transfers, localization, and data sovereignty across five Southeast Asian jurisdictions—Indonesia, Malaysia, Singapore, Thailand, and Vietnam—based on national laws, government regulations, and regulatory authority publications up to June 2025.)

Country	Regulations and Laws	Regulatory Body	Cross-Border Data Transfer	Data Localization	Data Protection	Data Sovereignty
Indonesia	Personal Data Protection Law 2022; GR 71/2019	Ministry of Communication and Information Technology (Kominfo); New PDP Authority (2024)	Allowed if adequate protection exists; fallback to binding safeguards or consent. Kominfo notification required.	No general mandate; required for public sector and certain sectors (e.g., finance).	Legal bases include consent, contract, legitimate interests. Mandatory DPO for large-scale processing. Breach notice within 72h.	Public sector data localized. Government access allowed for law enforcement. Foreign requests go through state.
Malaysia	Personal Data Protection Act 2010 (amended 2024)	Personal Data Protection Department (PDPD)	Allowed if receiving country ensures adequate protection or via consent. New TIA regime from 2025.	No general requirement; sector-specific (e.g., financial data).	Consent-based; data portability and mandatory DPO from 2025. Breach notification required.	Public sector exempt from PDPA. Government access allowed. No data export restrictions for sovereignty.
Singapore	Personal Data Protection Act 2012 (amended 2020); Cybersecurity Act 2018	Personal Data Protection Commission (PDPC)	Permitted with comparable protection, binding rules, or CBPR certification. No formal adequacy list.	No localization requirement; encouraged regional data hub.	Multiple legal bases including deemed consent and legitimate interest. Mandatory DPO. Breach notification within 72h.	No localization. Government access for law enforcement. Encourages data mobility with safeguards.
Thailand	Personal Data Protection Act 2019; Cybersecurity Act 2019	Personal Data Protection Committee (PDPC); National Cybersecurity Committee (NCSC)	Restricted to countries with adequate safeguards or with PDPC-approved BCR/SCC. Explicit consent acceptable.	No general requirement; sector-specific; cybersecurity laws provide broad access powers.	GDPR-like standards: legal bases include consent and legitimate interest. DPO required. Breach notification within 72h.	Government access via cybersecurity laws. Extraterritorial application asserts control over Thai citizen data.
Vietnam	Decree 13/2023 on Personal Data	Ministry of Public Security (MPS)	Strictly regulated:	Mandatory for certain sectors;	Consent-centric. DPO or DPD	Strongest sovereignty.

	Protection; Cybersecurity Law 2018; Data Law 2024		requires consent, Transfer Impact Assessment, and MPS approval.	foreign service providers must store user data locally under Cybersecurity Law.	required for sensitive/large-scale data. Breach notice to MPS within 72h.	Localization and prior approval for data transfers. Foreign government access blocked unless vetted.