SENSITIVE DATA AND PRIVACY PROTECTION IN THE MIDDLE EAST AND NORTH AFRICA BEYOND GENERAL DATA PROTECTION REGULATION (GDPR): LESSONS FOR BRUNEI

A. O. Salau*
A. O. Oyero**

ABSTRACT

This paper examines the evolving landscape of data protection and privacy regulations across the Middle East and North Africa (MENA region), with particular emphasis on approaches that diverge from the European Union's General Data Protection Regulation (GDPR). Through comparative analysis of legislative frameworks in key MENA jurisdictions, including the United Arab Emirates, Saudi Arabia, Egypt, and Morocco, this research identifies distinctive regional approaches to data sovereignty, religious and cultural considerations in privacy conceptualisation, and sector-specific regulatory models. The study contextualises these findings against Brunei Darussalam's current data protection framework, which remains in nascent stages of development having just come into force in early 2025. Drawing on the MENA region's experiences, this paper proposes a tailored roadmap for Brunei that balances international best practices with local legal traditions and cultural values. The findings suggest that Brunei might benefit from adopting elements of the UAE's free zone approach, Saudi Arabia's sector-specific regulations, and Morocco's balanced implementation strategy, while adapting these models to accommodate Brunei's unique socio-legal context and economic priorities.

Keywords: Data Protection, Privacy Regulation, MENA Region, Brunei, Comparative Law, GDPR, Digital Sovereignty

* Faculty of Law, Department of Jurisprudence & International Law, Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria
** Faculty of Law, Department of Public Law, Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria

INTRODUCTION

The global regulatory landscape for data protection and privacy has been profoundly influenced by the European Union's General Data Protection Regulation (GDPR), which came into effect in May 2018. While the GDPR has established itself as an influential benchmark, regions across the world have developed regulatory approaches that reflect their distinct legal traditions, cultural contexts, and economic priorities. The Middle East and North Africa (MENA) region presents a particularly rich and diverse case study in this regard, with countries adopting varied approaches to data protection that range from GDPR-inspired frameworks to more distinctive regulatory models[1]. Brunei Darussalam, a small but economically significant nation in Southeast Asia, stands at a critical juncture in developing its own approach to data protection and privacy. With its Wawasan (Vision) 2035 emphasising digital transformation and economic diversification, Brunei faces the challenge of establishing regulatory frameworks that both facilitate digital innovation and safeguard individual privacy rights (E-Government National Centre, 2020). It is expected that the nascent Brunei's Personal Data Protection Order, 2025 (PDPO 2025) would offer such robust protection.[2]

With the advent of digital economy, the process through which personal data is collected, considered, processed, and disseminated has been revolutionised. With this radical departure from the existing mode and the advent of a new one, transformation has become a parallel evolution in the governance of data, particularly in relation to the privacy and protection of individuals. The GDPR, enforced in 2018, represents a landmark in global data protection standards. Its influence extends beyond the EU, inspiring

[1] AM Al-Khouri, 'Data Protection Frameworks in the MENA Region: Evolution and Limitations' (2021) 6(2) Journal of Cyber Policy 175-194.

[2] See Brunei Darussalam Government Gazette No. S1 <https://www.agc.gov.bn/AGC%20Images/LAWS/Gazette_PDF/2025/EN/S%201_2025%20%5bE%5d.pdf> accessed 6 June 2025.

legislative developments in jurisdictions as diverse as Brazil, Japan, Kenya, and several states within the Middle East and North Africa (MENA) region[3].

However, the adaptation of such global standards often necessitates contextualisation. MENA states exhibit a wide range of legal systems, from civil law traditions to Sharia-based systems, and face unique political and socio-cultural challenges in implementing comprehensive data privacy frameworks. While some states, such as the United Arab Emirates (UAE) and Saudi Arabia, have introduced GDPR-like regulations, others lag due to institutional weaknesses, political instability, or prioritisation of state security over individual privacy.[4]

This paper examines how lessons from the MENA region's diverse approaches to data protection might inform Brunei's regulatory development. The research question guiding this study is: What elements of MENA region data protection frameworks, particularly those that diverge from the GDPR model, might offer valuable insights for Brunei's evolving data protection strategy? By examining jurisdictions with comparable legal traditions, cultural values, and development trajectories, this study aims to identify regulatory approaches that may be more contextually appropriate for Brunei than wholesale adoption of GDPR principles. The paper proceeds as follows: Section 2 examines the concept of GDPR taking into consideration its global reach. Section 3 reviews the existing literature on data protection frameworks in the MENA region taking some countries in the same region into consideration such as United Arab Emirates, Morocco, Saudi Arabia and Egypt while also considering Brunei. Section 4 outlines the methodology employed in this comparative analysis. Section 5 presents the findings, focusing on distinct features of MENA data protection

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

[4] Graham Greenleaf, 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance' (2021) 169 Privacy Laws & Business International Report 1, 3-5.

approaches. Section 6 discusses the implications of these findings for Brunei's regulatory development vis-à-vis the emergent PDPO 2025. Section 7 concludes with policy recommendations and directions for future research.

UNDERSTANDING GENERAL DATA PROTECTION REGULATION (GDPR) AND ITS GLOBAL REACH

The General Data Protection Regulation (GDPR) represents a paradigm shift in personal data protection within the European Union (EU) and beyond. It builds on the foundation laid by the 1995 Data Protection Directive, but unlike its predecessor, the GDPR is a regulation, directly applicable in all member states without the need for implementing national legislation. Its primary aim is to harmonise data protection laws across the EU while empowering individuals with greater control over their personal information.

At the heart of the GDPR are a set of foundational principles: lawfulness, fairness, and transparency; purpose limitation; data minimisation accuracy; storage limitation; integrity and confidentiality; and accountability. These principles guide the obligations of data controllers and processors, who must also adhere to lawful bases for data processing, ensure rights of access, rectification, and erasure (the 'right to be forgotten'), and facilitate data portability and objection rights for individuals.[5]

Extra- Territorial Scope and Global Implications

One of the most significant features of the General Data Protection Regulation (GDPR) is its extra-territorial applicability. Article 3(2) provides that the regulation applies to data controllers and processors outside the EU if they offer goods and services to, or monitor the behavior of, data subjects within the Union.[6] This has effectively exported European privacy

[5] Ibid.
[6] Bert- Jaap Kops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law Journal 250, 261-263.

standards to a global audience, compelling multinational corporations, and foreign governments alike to align their data handling practices with GDPR requirements.

Consequently, numerous countries have adopted the General Data Protection Regulation (GDPR) inspired reforms, including Brazil's Lei Geral De Protecao de Dado, South Korea's amendment to the Personal Information Protection Act.[7] These changes not only facilitate adequacy decisions under Article 4 of the General Data Protection Regulation which further reflects a global consensus around high standards of data protection across the globe.

The General Data Protection Regulation (GDPR) as a regulatory model beyond mere legal compliance, the GDPR has become a model for regulatory legitimacy, especially for emerging economies seeking to bolster their digital credibility. It serves as both a benchmark and a tool of digital diplomacy, often required for cross border trade agreement, cloud service, adoption, and digital trust frameworks.

However, adopting General Data Protection Regulation (GDPR) like laws present challenges in different legal and political contexts. The developing and authoritarian regimes must balance policy protection with the state's interest in surveillance, national security, or economic expediency.[8] The result is often a hybrid model; formal convergence with GDPR principles, but with exemptions or implementations gaps reflecting local priorities.

This dynamism is essentially evident in the Middle East and North Africa (MENA) regions where countries have adopted or proposed data protection laws with varying degree of GDPR influence. In assessing this development, it is expedient to account not only for textual similarities, but

[7] Greenleaf (n 4).
[8] Ibid.

also for the institutional, political, and cultural factors that shape enforcement and effectiveness.[9]

DATA PROTECTION FRAMEWORKS IN THE MENA REGION

The Middle East and North Africa region is currently undergoing significant transformation in her digital world, affected by expanding internet penetration and the existence of technological advancement applicable to areas of government and burgeoning technological sector. This paradigm shift in the digital world has sparked attentions towards data governance including privacy and protection. However, the region exhibits stark disparities in the arrears of legal development, enforcement capacity and political will regarding personal data protection.[10]

The MENA region is not a single entity as it encompasses monarchies, federal systems, republican and transitional government. These differences are reflected in regions legal systems, which draw from varieties of sources, including civil law, Islamic law, and mixed legal tradition.[11] Accordingly, privacy legislations vary widely in scope, form, and efficacy among countries in the Middle East North Africa.

It is however important to note that while many MENA governments maintain robust surveillance capabilities, often justified on grounds of national security and counterterrorism. In some cases, such as in Bahrain, Algeria, and Iran, state control over telecommunications infrastructure enables extensive data collection and monitoring.[12] These practices frequently undermine data privacy, even where formal laws exist. A 2018 report by Privacy International highlighted the prevalence of mass surveillance and lack of judicial oversight across the region, noting that laws

[9] Ibid.
[10] Privacy International, 'The State of Privacy in the Middle East and North Africa (2018)' <https://privacyinternational.org> accessed 25 April 2025.
[11] Chibli Mallat, *Introduction to Middle Eastern Law* (OUP 2007) 15-24.
[12] Access Now, 'Shattered Dreams and Lost Connections: Surveillance and Censorship in the MENA Region' (2019) <https://www.accessnow.org> accessed 25 April 2025.

granting sweeping surveillance powers are seldom balanced by meaningful safeguards or avenues for redress.[13] Consequently, data protection frameworks, where present, often serve as instruments of state legitimacy than genuine privacy guarantees.

Meanwhile, several MENA states have adopted or proposed data localisation policies, requiring that personal data be stored and processed within national borders. For Instance, Saudi Arabia's Cloud Computing Regulatory Framework and Egypt's Data Protection Law both impose restrictions on cross-border data transfers without prior approval.[14] These policies are frequently driven by concerns over foreign surveillance, economic sovereignty, and control over domestic data flows.

Invariably, data localisation may promote national cybersecurity and local capacity building. It can also hinder innovation, restrict global integration, and raise costs for businesses reliant on international cloud providers.[15] These tensions reflect broader debates over digital sovereignty and the role of the state in governing data ecosystems. A challenge which appears to assume a critical form across the MENA region is the weakness or absence of independent data protection authorities (DPAs). Where such bodies exist, they often lack the financial, technical, or legal capacity to enforce compliance. Morocco's National Commission for the Protection of Personal Data (CNDP) is among the few relatively active DPAs, while others remain underdeveloped or subordinate to executive control.[16]

The literature on data protection in the MENA region reveals a landscape characterised by regulatory diversity and rapid evolution. Scholars have documented the region's transition from minimal privacy regulation to

---

[13] Privacy International, 'The State of Privacy in the Middle East and North Africa (2018)' <https://privacyinternationa.org> accessed 25 April 2025.

[14] National Cybersecurity Authority (Saudi Arabia), Cloud Computing Regulatory Framework (2020); Egypt Law No. 151/2020 on Personal Data Protection, arts 2 & 14.

[15] Rolf H Weber, 'Data Location Requirements under Data Protection Law: A Legal and Economic Perspective' (2013) 2(1) International Data Privacy Law 27.

[16] Yasmeen Abutaleb, 'Morocco's CNDP and the Challenges of Data Governance in the Maghreb' (2021) 34 Journal of North African Studies 145.

increasingly comprehensive frameworks over the past decade.[17] Al-Khouri identifies three broad regulatory approaches within the region: GDPR-aligned comprehensive laws (exemplified by Morocco and Tunisia), hybrid models combining sectoral regulations with horizontal principles (Saudi Arabia and Egypt), and distinctive zone-based approaches (UAE).[18]

Several scholars have analysed the distinctive features of MENA data protection frameworks. Rahman highlights how Islamic legal principles, including concepts of inviolability and privacy have influenced regional approaches to personal data.[19] Bensemmane and others document how considerations of national security and data sovereignty have shaped regulatory frameworks, particularly in Gulf Cooperation Council (GCC) countries.[20] El-Zoheiry examines how cultural attitudes toward privacy in various MENA jurisdictions have resulted in distinctive provisions regarding sensitive data categories, consent requirements, and enforcement mechanisms. Literature also acknowledges significant variation within the region.[21] Greenleaf and Cottier note the contrast between Morocco's GDPR-aligned approach and the UAE's free zone model, which establishes distinct regulatory regimes for specific economic zones.[22] Maldonado and Sybel analyse Saudi Arabia's sector-specific approach, which has developed detailed regulations for healthcare, financial services, and telecommunications while maintaining broader principles for other sectors.[23]

---

[17] G Greenleaf and B Cottier, 'Comparing Data Privacy Laws: GDPR v. MENA Frameworks' (2020) 163 Privacy Laws & Business International Report 15-17.
[18] Al-Khouri (n 1).
[19] F Rahman, 'Islamic Perspectives on Data Protection: Hurma and Khususiyya in the Digital Age' (2019) 3(2) Journal of Islamic Ethics 207-229.
[20] S Bensemmane, A Al-Saud and F Rahman 'National Security and Data Sovereignty: Comparative Perspectives from the Gulf Cooperation Council' (2022) 30(1) International Journal of Law and Information Technology 23-46.
[21] A El-Zoheiry, 'Cultural Dimensions of Data Protection in the Middle East' (2020) 38 Computer Law & Security Review 105-121.
[22] Greenleaf and Cottier (n 17).
[23] J Maldonado and C Sybel, 'Saudi Arabia's Sectoral Approach to Data Protection: Comparative Analysis and Implementation Assessment' (2023) 13(1) International Data Privacy Law 42-59.

Brunei's Current Data Protection Landscape

Research on Brunei's data protection framework remains relatively limited. Even Mahmod's comprehensive analysis, describing Brunei's current approach as 'emergent and sectoral' was based on the position prior to coming into force of the draft Personal Data Protection Order 2016. Then, Brunei's data specific provisions were scattered across telecommunications regulations, financial services directives, and healthcare standards.[24] Teo examines Brunei's approach to data protection through the lens of its Wawasan 2035 development agenda, arguing that the nation faces a tension between ambitious digitisation goals and underdeveloped privacy frameworks.[25] Similarly, Duraman and Hashim highlight how Brunei's aspiration to develop a digital economy has created pressure for more robust data protection regulations that align with international standards while respecting local legal traditions.[26] Several scholars have contextualised Brunei's data protection challenges within its distinctive legal system. Hashim explores how Brunei's dual legal system, which incorporates both civil law and Sharia principles, creates unique considerations for privacy regulation.[27] Similarly, Wong analyses how Malay Islamic Monarchy (MIB) principles, which form the foundation of Brunei's national philosophy, might influence conceptualisations of privacy and data protection in ways that diverge from Western models.[28]

---

[24] Z Mahmod, 'Data protection in Brunei Darussalam: Current Status and Future Directions' (2022) 9(1) Asian Journal of Law and Society 123-142.

[25] S Teo Wawasan, '2035 and Digital Transformation: Privacy Challenges in Brunei Darussalam' (2021) 23(3) Digital Policy, Regulation and Governance 267-284.

[25] F Wong Malay, 'Islamic Monarchy and Modern Data Governance: Reconciling Tradition and Innovation in Brunei Darussala' (2020) 9(2) Southeast Asian Studies 189-210.

(2021).

[26] I Duraman and H Hashim 'Digital Economy Aspirations in Brunei Darussalam: Policy Challenges and Regulatory Imperatives' (2020) 37(3) ASEAN Economic Bulletin 312-330.

[27] H Hashim, 'Dual Legal Systems and Regulatory Compliance: Data Protection in Brunei Darussalam' (2019) 15(2) Journal of Islamic Law and Comparative Jurisprudence 78-96.

[28] Malay (n 25).

While the General Data Protection Regulation (GDPR) sets a high standard for personal data protection, its adoption and adaptation in MENA countries reflect both legal convergence and contextual divergence. The following section compares key GDPR features with those found in MENA data protection frameworks, focusing on five core areas: consent and individual rights, lawful bases for processing, data transfers and localisation, enforcement mechanisms, and cultural-political context.

Consent and Data Subject Rights

Under the GDPR, consent must be freely given, specific, informed, and unambiguous.[29] It is one of six lawful bases for data processing but cannot be presumed or coerced. Additionally, the GDPR enshrines comprehensive rights for data subjects, including the rights to access, rectification, erasure, restriction, objection, and data portability.

Several MENA laws, such as those in the UAE, Egypt, and Saudi Arabia echo these principles, requiring affirmative consent and granting data subjects basic rights.[30] However, there are notable limitations. In many jurisdictions, the scope of rights is narrower, and enforcement mechanisms to ensure the exercise of those rights are weak or undefined. For instance, Egypt's law provides for data subject rights, but implementation delays and regulatory ambiguity have rendered these provisions largely aspirational.[31]

Lawful Basis for Processing

The GDPR permits data processing under several legal bases, including consent, contractual necessity, legal obligations, protection of vital interests, performance of a public task, and legitimate interests. This multifaceted approach balances flexibility with accountability. In contrast, MENA laws tend to centre on consent as the primary or sole lawful basis for processing, often lacking explicit provisions for other bases such as legitimate interest

[29] Bensemmane, Al-Saud and Rahman (n 20).
[30] Ibid.
[31] Access Now, 'Egypt's New Data Protection Law: Progress or More State Control?' (2020) <https://www.accessnow.org> accessed 26 April 2025.

or public task. This narrow approach may lead to over-reliance on consent and weaken the robustness of legal justifications in sectors such as healthcare, finance, or public administration.

Data Transfers and Localisation

One of the GDPR's most complex areas involves cross-border data transfers. Articles 44–50 provide mechanisms for international transfers, including adequacy decisions, standard contractual clauses (SCCs), and binding corporate rules (BCRs).[32] These instruments aim to ensure that EU personal data remains protected, regardless of its destination. In the MENA region, however, several countries have imposed strict localisation requirements or established burdensome procedures for data exports. Saudi Arabia, prior to its 2023 amendments, prohibited almost all international transfers. Egypt mandates prior approval from the regulator for any outbound transfers.[33] While framed as protective, these policies often serve economic or security purposes and may conflict with global digital trade norms.

Enforcement Mechanisms and Sanctions

The GDPR grants significant powers to independent supervisory authorities, including investigative and corrective powers, the ability to impose administrative fines (up to €20 million or 4% of global turnover), and mandates cooperation through the European Data Protection Board (EDPB).[34] MENA enforcement structures are generally weaker. While some countries have established data protection authorities (e.g., UAE's Data Office, Morocco's CNDP), their independence, resources, and enforcement records vary widely. In Egypt and Saudi Arabia, regulators are embedded within government ministries or executive bodies, limiting their autonomy.[35] Moreover, sanctions tend to be modest, and litigation is rare

[32] Ibid.
[33] Ibid.
[34] Bensemmane, Al-Saud and Rahman (n 20).
[35] Ibid.

due to weak judicial traditions in administrative or constitutional rights enforcement.

Cultural and Political Contexts

GDPR's emphasis on individual autonomy and transparency presumes liberal democratic governance and an engaged civil society. In MENA, however, collective norms, state-led development, and limited press freedom create challenges for data protection as a rights-based agenda. Surveillance, censorship, and political control over digital spaces are often prioritised over individual privacy.

While existing research offers valuable insights into both MENA data protection frameworks and Brunei's regulatory landscape, significant gaps remain. First, comparative analyses specifically examining the relevance of MENA approaches for Brunei are notably absent. Second, much of the literature focuses on comparing regional frameworks to the GDPR rather than identifying distinctive elements that might offer alternative regulatory models. Third, few studies consider how cultural and religious similarities between MENA countries and Brunei might inform contextually appropriate data protection strategies. This paper aims to address these gaps by conducting a focused comparative analysis of MENA data protection approaches that diverge from the GDPR model, with specific attention to their potential relevance for Brunei's regulatory development.

However, while MENA laws may replicate GDPR language, their underlying philosophies and implementation realities differ. This creates what scholars have termed "legal transplant fatigue" – where laws are adopted for legitimacy rather than functionality.[36]

[36] Pierre Legrand, 'The Impossibility of "Legal Transplants"' (1997) 4 Maastricht Journal of European and Comparative Law 111.

METHODOLOGY

This study employs a qualitative comparative analysis of data protection frameworks in selected MENA jurisdictions and Brunei. The research design prioritises depth over breadth, focusing on four MENA jurisdictions – the United Arab Emirates, Saudi Arabia, Egypt, and Morocco – that represent diverse regulatory approaches while sharing certain contextual similarities with Brunei.

Jurisdiction Selection

The selection of jurisdictions was guided by three criteria: regulatory diversity, contextual relevance to Brunei, and data availability. The UAE was selected for its innovative free zone approach and its position as a regional hub for digital economy development, paralleling Brunei's economic diversification aspirations. Saudi Arabia represents a monarchy with a dual legal system incorporating civil law and Sharia principles, similar to Brunei's legal structure. Egypt offers insights from a jurisdiction balancing data protection with significant security considerations, while Morocco provides an example of GDPR adaptation within a distinctive cultural context.

Data Sources

The study draws on three primary data sources: (1) legal texts, including laws, regulations, and regulatory guidelines from each jurisdiction; (2) regulatory decisions and enforcement actions that illustrate how legal frameworks operate in practice; and (3) expert commentaries from legal practitioners, academics, and regulatory authorities. All documents were analysed in either their original English form or through official translations.

Analytical Framework and Limitations

The analysis employs a structured comparison framework focused on five dimensions of data protection regulation: (1) Regulatory architecture

(comprehensive vs. sectoral approaches); (2) Jurisdictional scope and data localisation requirements; (3) Definitions and categories of sensitive data; (4) Consent mechanisms and individual rights; and (5) Enforcement structures and penalties. For each dimension, the analysis identifies both convergence with GDPR principles and distinctive elements that represent alternative regulatory approaches. Particular attention is given to provisions that reflect religious principles, cultural values, economic priorities, or security considerations specific to the MENA context. However, the study faces several methodological limitations that warrant acknowledgement. First, the rapid evolution of data protection frameworks in both the MENA region and Brunei means that specific provisions may change and have indeed changed during the research period such as the coming into force of Brunei's PDPO 2025. Second, the analysis of legal texts may not fully capture implementation realities, particularly in jurisdictions where enforcement practices are still developing. Third, linguistic and translation limitations may affect interpretation of certain legal nuances, despite efforts to utilise official translations and expert commentaries.

FINDINGS: DISTINCTIVE FEATURES OF MENA DATA PROTECTION APPROACHES

The comparative analysis identified several distinctive features of MENA data protection frameworks that diverge from the GDPR model and may offer relevant insights for Brunei's regulatory development.

Free Zone and Sectoral Regulatory Models

Unlike the GDPR's comprehensive horizontal approach, several MENA jurisdictions have developed distinctive regulatory architectures that create differentiated data protection regimes for specific sectors or zones. In Saudi Arabia, banking law requires customer data to be stored within the country, while payment services and electronic money institutions must locate all primary and secondary IT systems domestically.[37] The UAE's financial free

[37] securiti, 'Data Regulations in Saudi Arabia's Financial Sector' <https://securiti.ai/data-regulations-in-saudi-arabia-financial-

zone model represents the most developed example, with the Dubai International Financial Centre (DIFC) and Abu Dhabi Global Market (ADGM) establishing their own data protection regimes that apply exclusively within their jurisdictional boundaries. These are respectively DIFC Data Protection Law No. 5 of 2020 and Data Protection Regulations 2020 (as amended) (effective 1 July 2020) and ADGM Data Protection Regulations 2021.[38] While these free zone regulations often incorporate GDPR-inspired provisions, they adapt them to the specific economic activities and institutional contexts of each zone. For instance, the DIFC Data Protection Law 2020 maintains GDPR principles regarding data minimisation and purpose limitation but establishes more flexible rules for data transfers to facilitate the Centre's role as a regional financial hub.[39]

In the case of the United Arab Emirates, the UAE introduced Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, the country's first comprehensive data protection law at the federal level.[40] The law draws heavily on GDPR principles, including requirements for lawful processing, consent, data subject rights, and data breach notification. It establishes the UAE Data Office as the primary regulatory authority and provides for extraterritorial application to data processing activities affecting UAE residents. However, despite its alignment with international norms, the law contains vague provisions regarding government data and potential exemptions for national security, which may limit its enforcement scope. Moreover, the UAE's complex regulatory structure comprising free

sector/#:~:text=Financial%20institutions%20are%20expected%20to%20safeguard%20sensitive,Protection%20Standards%20(NDMO%20standards)%20and%20the%20CIL> accessed 12 June 2025.

[38] See *OneTrust DataGuidance* 'Jurisdiction Dubai International Financial Centre' <https://www.dataguidance.com/jurisdictions/united-arab-emirates-dubai-international-financial-centre> accessed 6 June 2025; DLA DIPER 'Data protection laws in UAE - Abu Dhabi Global Market Free Zone' <https://www.dlapiperdataprotection.com/?t=law&c=AE4> accessed 6 June 2025.

[39] See *Onetrust DataGuidance*, 'Comparing Privacy Laws: GDPR v. DIFC Law 2007 and 2020' <https://www.dataguidance.com/sites/default/files/gdpr_v_difc_law.pdf> accessed 6 June 2025.

[40] Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE).

zones like DIFC ADGM, each with its own data laws – creates jurisdictional complexity.[41]

Regarding healthcare data governance, the UAE's sovereign cloud solutions ensure sensitive patient data is stored and processed within UAE borders, meeting strict national and international requirements on data residency and security.[42] Similarly, Saudi Arabia has developed sector-specific regulations for healthcare data (through the Saudi Health Information Exchange Policy) and financial information (through Saudi Central Bank directives) alongside broader principles contained in the Essential Cybersecurity Controls.[43] This approach differs significantly from the GDPR's uniform application across sectors and jurisdictions, offering a more flexible and contextualised regulatory model that may be particularly relevant for economies in transition.

Consequently, Saudi Arabia enacted the Personal Data Protection Law (PDPL) in 2021, subsequently amended in 2023 to address compliance challenges and facilitate cross-border data flows.[44] Administered by the Saudi Data and Artificial Intelligence Authority (SDAIA), the PDPL is designed to support the Kingdom's Vision 2030 goals and promote digital transformation.[45] The law defines key rights and obligations, including

---

[41] ADGM Data Protection Regulations 2021; DIFC Law No. 5 of 2020 (Data Protection Law); see also Martin Molloy, 'Data Protection Laws in the UAE: DIFC, ADGM and Federal Contrasts' (2022) 38 Journal of International Commercial Law 115.

[42] Inas Al Khatib, Norhan Ahmed and Malick Ndyiaye, 'GDPR Compliance of Hospital Management Systems in the UAE' 2024 00(00) Journal of Data Science and Intelligent Systems 1-14.

[43] ICLG, 'Data Protection Laws and Regulations Saudi Arabia 2024-2025 <https://iclg.com/practice-areas/data-protection-laws-and-regulations/saudi-arabia> accessed 12 June 2025; Nada Saddig Almaghrabi1 and Bussma Ahmed Bugis 'Patient Confidentiality of Electronic Health Records: A Recent Review of the Saudi Literature' (2022) Dr. Sulaiman Al Habib's Medical Journal https://doi.org/10.1007/s44229-022-00016-9.

[44] Saudi Arabia, Personal Data Protection Law (2021, as amended 2023); see also SDAIA, 'Regulations and Guidelines on Personal Data' <https://sdaia.gov.sa> accessed 24 April 2025.

[45] Nick O'Connell, 'CITC's New Cloud Computing Regulatory Framework in Saudi Arabia' <https://www.tamimi.com/law-update-articles/citcs-new-cloud-computing-regulatory-framework-in-saudi-

consent-based processing, data subject rights, and breach reporting. However, the original version's strict localisation requirements were relaxed in the 2023 amendments, allowing cross-border transfers with regulatory approval.[46] Nonetheless, ambiguities regarding state access to data and limited independence of the supervisory authority continue to raise concerns among privacy advocates.

Similarly, Egypt passed Law No. 151 of 2020, the Personal Data Protection Law, which aims to regulate the collection, storage, and processing of personal data.[47] It mandates data subject consent, introduces cross-border transfer restrictions, and provides for the establishment of a Personal Data Protection Centre under the Ministry of Communications and Information Technology.[48] While the law adopts many GDPR-like features, concerns have been raised over its vague definitions, limited independence of the regulator, and potential misuse for state surveillance.[49] The law's implementation also remains incomplete, with key executive regulations and institutional appointments pending as of 2025. Morocco also has her data protection framework is grounded in Law No. 09-08 adopted in 2009, which regulates the processing of personal data and establishes the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP).[50] The law was among the earliest in Africa to reflect European privacy norms, owing to Morocco's association with the EU through trade and cooperation agreements.

---

arabia/#:~:text=Following%20public%20consultation%20in%202016%2C%20Saudi%20Arabia%27s,of%20cloud%20computing%20services%20in%20the%20Kingdom> accessed 12 June 2025.

[46] Noura Al-Mutairi, 'The Evolution of Data Localization in Saudi Law: Implications for the Private Sector' (2024) Middle East Law and Governance.

[47] Sarie Eldin & Partners, 'Law No. 151 of 2020 promulgating the Personal Data Protection Law' <https://sarieldin.com/sites/default/files/2023-03/LexisNexis%20Update%20-%20August%202020.pdf> accessed 12 June 2025.

[48] Ibid.

[49] Access Now, 'Egypt's New Data Protection Law: Progress or More State Control?' (2020) <https://www.accessnow.org> accessed 21 April 2025.

[50] Morocco Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data.

However, the CNDP has engaged in public awareness campaigns, issued compliance guidance, and processed complaints. Nevertheless, enforcement remains constrained by institutional limitations and political sensitivities.[51] Morocco is seeking an adequacy decision from the EU, which has prompted discussions on reforming its legislation to align more closely with GDPR standards. The forgoing sophisticated sector-specific regulatory approaches could inform Brunei's implementation of its data protection regime.

Data Sovereignty and Localisation Requirements.

MENA jurisdictions have generally adopted more assertive and sophisticated but varied approaches to data sovereignty than the GDPR, with several countries implementing strict data localisation requirements for specific data categories that offer valuable insights for Brunei. Saudi Arabia has implemented one of the most comprehensive data localisation regimes, with certain categories of critical and sensitive data required to be stored and processed within the country, overseen by the National Data Management Office (NDMO). The Saudi PDPL, which became fully enforceable in September 2024, includes specific transfer regulations requiring adequate protection levels or appropriate safeguards like standard contractual clauses or binding corporate rules. Egypt's Personal Data Protection Law No. 151 of 2020 prohibits the transfer of personal data to foreign jurisdictions without explicit regulatory approval, with particularly stringent requirements for data deemed critical to national security or economic interests.[52] It requires organisations to obtain authorised licenses from the Personal Data Protection Center for processing activities, with maximum fees reaching 2,000,000 Egyptian Pounds (approximately US$125,000). This represents a significant departure from consent-based models. Morocco's Law No. 09-08, enacted in 2009, was among the first in the region to align with the modernised Convention 108+, establishing the

[51]Yasmeen Abutaleb, 'Morocco's CNDP and the Challenges of Data Governance in the Maghreb' (2021) 34 Journal of North African Studies 145.
[52] Sarie Eldin & Partners (n 47).

National Commission for the Protection of Personal Data (CNDP) as an independent regulator.[53]

Similarly, Saudi Arabia's Cloud Computing Regulatory Framework requires that certain categories of sensitive data, including government data and health records, must be physically stored within national boundaries.[54] The UAE operates a complex three-tier jurisdictional system with Federal Decree Law No. 45 of 2021 involving federal-level restrictions on cross-border data transfers applying to the mainland, whilst DIFC and ADGM economic free zones maintain their own more flexible GDPR-aligned regulations.[55] This creates what practitioners describe as 'sophisticated regulatory arbitrage' where businesses can choose their most appropriate jurisdiction based on operational needs. These provisions reflect a conceptualisation of data as a national resource requiring sovereign control, contrasting with the GDPR's emphasis on ensuring adequate protection regardless of data location. This sovereignty-focused approach may offer relevant perspectives for smaller nations like Brunei seeking to maintain control over critical data resources while participating in global digital ecosystems.

Religious and Cultural Influences on Privacy Conceptualisation

A particularly distinctive feature of MENA data protection frameworks is their incorporation of religious and cultural concepts into legal definitions of privacy and sensitive data. According to Islamic doctrine, every aspect of life is deemed private unless shown otherwise, with the public sphere limited to areas where governmental authority operates transparently. Islamic law traditionally recognises privacy as a fundamental concept, with the private sphere inhabited exclusively by an individual and the divine. Several MENA privacy laws generally follow Islamic legal principles and are based on personal privacy rights outlined in national constitutions, with

---

[53] Data Protection Africa, 'Morocco Data Protection Factsheet' <https://dataprotection.africa/morocco/> accessed 12 June 2025.
[54] O'Connell (n 45).
[55] See Data Protection Law DIFC Law No. 5 of 2020.

explicit consent required for processing sensitive personal data revealing religious beliefs or ethnic origin. Relatedly, MENA region's diversity means cultural and social factors play crucial roles in shaping how data privacy laws are interpreted and enforced, requiring organisations to be aware of nuances when undertaking data processing and handling sensitive data to avoid unintentional breaches of cultural norms.

For instance, Saudi Arabia's regulatory guidance on data protection cites the Quranic concept of 'hurma' (inviolability) as a foundational principle justifying protection of personal information.[56] Similarly, Morocco's Data Protection Law 09-08 includes specific provisions regarding the protection of data revealing religious practices and beliefs, reflecting the cultural significance of religious identity in Moroccan society.[57] Egypt's Personal Data Protection Law (Law No. 151 of 2020), extends special protection to data that might affect 'family honour' or 'religious reputation', categories not explicitly recognised in the GDPR framework.[58] These provisions demonstrate how religious and cultural values can shape data protection frameworks in ways that diverge from Western models, potentially offering insights for Brunei's efforts to develop regulations aligned with its Malay Islamic Monarchy principles.

Pragmatic Implementation Strategies

MENA jurisdictions have generally adopted more gradual and pragmatic implementation approaches than the GDPR's relatively rapid and comprehensive rollout. Morocco's data protection authority (CNDP) has employed a 'progressive compliance' model, working with different sectors to develop tailored implementation timelines and focusing enforcement

[56] Rahman (n 19).
[57] Kingdom of Morocco Administration of National Defense General Directorate of Information Systems Security, 'Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data' <https://www.dgssi.gov.ma/en/loi-09-08-relative-la-protection-des-personnes-physiques-legard-du-traitement-des> accessed 12 June 2025.
[58] Bensemmane, Al-Saud and Rahman (n 20).

actions on educational rather than punitive measures during initial phases.[59] This approach has resulted in higher voluntary compliance rates while avoiding the compliance burden that accompanied the GDPR's implementation.[60] Similarly, the UAE's free zone authorities have adopted a consultative approach to regulatory development, with multiple rounds of industry feedback shaping both substantive requirements and implementation timelines. The DIFC Data Protection Law 2020 included a 12-month grace period for existing businesses, with additional extensions for specific requirements based on organisational size and complexity.[61] These implementation strategies reflect a recognition of the capacity constraints facing organisations in emerging digital economies, offering potential lessons for Brunei's transition toward more comprehensive data protection.[62]

In the final analysis, the MENA experience demonstrates that successful data protection frameworks require careful balancing of international standards, cultural considerations, and national sovereignty objectives. Brunei's unique position as both an Islamic state and ASEAN member creates opportunities to develop an innovative framework that could serve as a model for other Muslim-majority developing nations navigating similar challenges.

---

[59] Paradigm Initiative and Omidya Network, 'Data Protection Authorities (DPAs) in Africa: A Report on the Establishment, Independence, Impartiality and Efficiency of Data Protection Supervisory Authorities in the Two Decades of their Existence on the Continent' <https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-2.pdf#:~:text=This%20report%20comes%20at%20an%20important%20time%2C,and%20efficiency%20of%20data%20protection%20supervisory%20authorities> accessed 12 June 2025.

[60] For instance, Saudi Arabia, see Data Management Office, 'National Data Governance Interim Regulations 1 June 2020' <https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf> accessed 12 June 2025.

[61] DIFC, 2020.

[62] Greenleaf and Cottier (n 17).

IMPLICATIONS FOR BRUNEI'S REGULATORY DEVELOPMENT

The distinctive features of MENA data protection approaches identified above offer several potential insights for Brunei's evolving regulatory framework. This section discusses the implications of these findings in the context of Brunei's specific legal, cultural, and economic circumstances. The implications of MENA data protection approach for Brunei should be assessed after first considering the strengths of Brunei's PDPO 2025, i.e., to what extent has the Order addressed the concerns.

Brunei's PDPO 2025: An Overview

Endorsed by the Sultan of Brunei Darussalam on 8 January 2025, Brunei's PDPO 2025 creates a comprehensive framework of 12 parts, 65 articles and 6 schedules (elaborating on varied individual, public and national security interests),[63] to govern the processing in terms of collection, storage, use, disclosure, erasure, etc., of personal data by organisations.[64] In line with international standards, it defines "personal data" to mean any data, whether true or not, about an individual who can be identified.[65] The Order applies only to private sector organisations and NGOs, with government entities operating under existing frameworks including Data Sharing Guidelines and the Official Secrets Act.[66] The PDPO lays down several GDPR-like principles of data processing such as informed consent, purpose limitation, the obligations of data processors, and comprehensive rights of individuals

[63] Brunei Darussalam Government Gazette, 'Personal Data Protection Order, 2025' <https://www.agc.gov.bn/AGC%20Images/LAWS/Gazette_PDF/2025/EN/S%201_2025%20%5bE%5d.pdf> accessed 12 June 2025.
[64] PDPO 2025, art 1(3) & 2.
[65] PDPO 2025, art 2.
[66] Rasidah Hj Abu Bakar, 'Brunei Enacts New Law Giving Citizens Control Over Personal Data: The Sultanate's Landmark Data Privacy Law Takes Effect' (*The Scoop*) <https://thescoop.co/2025/03/08/brunei-enacts-new-law-giving-citizens-control-over-personal-data/#:~:text=While%20the%20PDPO%20applies%20only%20to%20private,Secrets%20Act%2C%20and%20the%20Protective%20Security%20Manual.&text=The%20PDPO%20also%20safeguards%20against%20data%20misuse,and%20implement%20protocols%20for%20managing%20data%20breaches> accessed 12 June 2025.

including to access, withdraw consent, correct and remedies (civil and criminal), e.g., for data loss, damage, unauthorised disclosure, etc.[67] Importantly, article 60 references article 18 and prescribes the duty to preserve secrecy of personal data as may be required while article 24 prohibits the unauthorised transfer of personal data outside Brunei to another country without a comparable standard of protection. The Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) established by section 3 of the Authority for Info-communications Technology Industry of Brunei Darussalam Order, 2001 serves as the primary regulatory authority, and invested with humongous advisory, rulemaking, investigative, promotional, penal, technical and other powers.[68]

Potential Application of Free Zone and Sectoral Models

Given that the PDPO applies to private sector organisations handling data for public entities, though government agencies are still obligated to manage personal data responsibly, Brunei should consider developing differentiated requirements for financial services, healthcare, and government sectors. Brunei's economic diversification strategy, focused on developing specific sectors including Islamic financial services, eco-tourism, and business process outsourcing, may benefit from the zone-based or sectoral regulatory approaches observed in the UAE and Saudi Arabia. Rather than implementing a uniform GDPR-style framework across all sectors, Brunei could consider developing tailored data protection regimes for priority economic areas. For instance, the Brunei Economic Development Board has established the Brunei Research and Development Centre, which could function as a regulatory sandbox for data-intensive innovation with specific privacy rules, similar to the UAE's free zone model.[69]

Similarly, Brunei's aspiration to become a hub for Islamic financial services might warrant sector-specific data protection provisions that address the

[67] PDPO 2025, arts 8-20, 21-28, 30-33, & 59.
[68] PDPO 2025, Part 2.
[69] Duraman and Hashimm (n 22).

unique requirements of Sharia-compliant financial instruments.[70] This approach would allow Brunei to balance comprehensive protection with the flexibility needed to facilitate digital innovation in target sectors. However, it would require careful coordination to avoid regulatory fragmentation and ensure consistent baseline protections across the economy.

Balancing Data Sovereignty and International Integration

Brunei faces the challenge of maintaining sovereign control over sensitive data while participating in international digital ecosystems. While MENA jurisdictions focus heavily on data sovereignty, Brunei's membership in ASEAN creates opportunities for regional data flow frameworks that balance sovereignty with economic integration. Hence, Brunei should consider developing explicit data localisation requirements for critical sectors but tailored to Brunei's economic priorities and its regional integration commitments. The data localisation approaches adopted by Egypt and Saudi Arabia offer potential models, particularly given Brunei's limited domestic capacity for data storage and processing.[71] A balanced approach might involve identifying specific data categories requiring domestic storage (such as government records, critical infrastructure data, and sensitive health information) while establishing clear mechanisms for responsible cross-border transfers of commercial and non-sensitive data. This could be complemented by regional data-sharing agreements, potentially within the ASEAN framework, that establish mutual recognition of data protection standards.[72] Brunei might also consider the UAE's approach of establishing specific data corridors with key economic partners, creating streamlined mechanisms for data transfers to jurisdictions with established adequacy arrangements. Given Brunei's significant economic

[70] El-Zoheiry (n 21).
[71] Digital Economy Council, Brunei Darussalam, *Digital Economy Masterplan 2025* (2020) <https://www.mtic.gov.bn/DE2025/documents/Digital%20Economy%20Masterplan%202025.pdf> accessed 12 June 2025.
[72] Mahmod (n 24).

relationships with Singapore, Malaysia, and Japan, such arrangements could facilitate digital trade while maintaining appropriate protections.

Incorporating Religious and Cultural Values

Brunei's legal system is dualistic, comprising civil laws and an increasingly assertive Sharia-based legal regime, particularly in criminal matters.[73] While Sharia values emphasise dignity, modesty, and the protection of private life, there is currently no direct application of these principles in the context of personal data regulation. Nonetheless, the cultural and religious context may offer a normative foundation for data privacy, especially where it aligns with Islamic ethical teachings on safeguarding information and preventing harm. This could provide an indigenous rationale for privacy protection that complements international standards like the GDPR.[74] Given Brunei's status as an Islamic state with similar cultural foundations, the kingdom could benefit from explicitly incorporating Islamic privacy principles into its data protection framework, for handling religiously sensitive data, potentially providing stronger cultural legitimacy and acceptance.

Brunei's national philosophy of Malay Islamic Monarchy (MIB) provides a distinctive cultural and religious context for conceptualising privacy and data protection. The examples from Saudi Arabia[75] and Morocco demonstrate how Islamic legal principles, and cultural values can be incorporated into regulatory frameworks without compromising fundamental protection standards. Brunei's data protection framework could explicitly reference relevant Islamic concepts such as 'hurm' (inviolability) and 'amanah' (trust) as foundational principles justifying data protection.[76]

---

[73] Ann Black and Hossein Esmaeili, *Modern Perspectives on Islamic Law* (Edward Elgar 2023) 142-145.
[74] Mohammad Hashim Kamali, *Privacy and Data Protection in Islamic Law* (International Institute of Advanced Islamic Studies 2019) 7-10.
[75] Maldonado and Sybel (n 23).
[76] Hashim (n 27).

Similarly, the definition of sensitive data categories could reflect specific cultural and religious sensitivities in Bruneian society, potentially extending special protection to information regarding religious practices, family relationships, or other culturally significant domains. This culturally grounded approach would likely enhance the legitimacy and effectiveness of data protection regulations by aligning them with existing normative frameworks. However, it would require careful balancing to ensure compatibility with international standards necessary for cross-border data flows.

Adopting Pragmatic Implementation Strategies

Given Brunei's relatively small market size and the limited data protection expertise available domestically, the progressive implementation strategies observed in Morocco and the UAE may be particularly relevant. Rather than attempting comprehensive implementation of a GDPR-style framework, Brunei might benefit from a phased approach that prioritises critical sectors and high-risk data processing activities. This could involve establishing baseline principles applicable across all sectors while developing more detailed regulations for priority areas such as healthcare, financial services, and telecommunications. Implementation timelines could be tailored to organisational capacity, with larger entities and critical sectors facing earlier compliance deadlines. Brunei's Digital Economy Masterplan 202 outlines several strategic goals, including enhancing digital infrastructure, fostering digital innovation, and ensuring cybersecurity and trust. Notably, the Masterplan identifies data governance and "privacy protection" as essential to building user confidence in digital services.[77]

However, these aspirations remain aspirational without corresponding legislative action. In the absence of a regulatory authority with data protection oversight effective implementation will be hindered. The AITI of Brunei Darussalam established by section 3 of the Authority for Info-communications Technology Industry of Brunei Darussalam Order, 2001 is

[77] Digital Economy Council, Brunei Darussalam (n 71) 32.

Brunei central body empowered to monitor data practices and adjudicate complaints.[78] A consultative approach by the Authority to regulatory development, similar to that employed in the UAE's free zones, would also allow Brunei to benefit from international expertise while ensuring that regulations address local circumstances. This might include public-private working groups focused on specific sectors or data categories; pilot implementation programmes with selected organisations, and regular revision of regulatory guidance based on implementation experiences. Brunei could enhance AITI's capabilities through partnerships with established regulators like Saudi Arabia's SDAIA or UAE's Data Office.

CONCLUSION AND RECOMMENDATIONS

This paper has examined distinctive features of data protection frameworks in the MENA region and their potential relevance for Brunei's regulatory development. As Brunei continues to develop its data protection framework, the experiences of MENA jurisdictions offer valuable lessons in balancing international standards with local contexts. By adopting elements of the UAE's free zone approach, Saudi Arabia's incorporation of Islamic principles[79] and Morocco's progressive implementation strategy, Brunei has the opportunity to establish a distinctive regulatory model that protects individual privacy while facilitating its digital economy aspirations. Rather than viewing the GDPR as the only viable template for data protection, policymakers should recognise the value of diverse regulatory approaches that reflect specific historical, cultural, and economic circumstances.

For Brunei, a thoughtfully adapted framework that draws on relevant international experiences while respecting local traditions may ultimately prove more effective than wholesale adoption of European models. The findings suggest that while the GDPR offers valuable principles for data

[78] PDPO 2025, arts 34-40.

[79] National Cybersecurity Authority, Saudi Arabia, 'Guide to Essential Cybersecurity Controls (ECC) Implementation' (2025) <https://nca.gov.sa/en/regulatory-documents/guidelines-list/gecc/> accessed 12 June 2025.

protection, alternative regulatory models from the MENA region may provide insights more aligned with Brunei's specific legal, cultural, and economic context. As Brunei continues its journey towards becoming a leading digital economy in Southeast Asia, the development of a comprehensive data protection framework appears to be essential. Noting the experiences of the Middle East and North Africa (MENA) region, this article has highlighted key lessons that can guide Brunei in the implementation of her new PDPO Order 2025 in aligning with international best practices while remaining culturally and contextually relevant.

Based on the comparative analysis conducted in this study, several specific recommendations emerge for Brunei's data protection strategy, these strategies and methodologies if considered and followed as recommended would make Brunei as a country advance in the area of data protection and keep it leading in such. Brunei authorities should therefore consider doing the following:

a) Adopt a hybrid regulatory architecture that combines horizontal baseline principles with sector-specific regulations for priority areas such as financial services, healthcare, and telecommunications. This approach would provide comprehensive protection while allowing for contextualised implementation.

b) Consider a zone-based approach for initiatives such as the Brunei Research and Development Centre, establishing specific data governance regimes that facilitate innovation while maintaining appropriate protections.[80]

c) Develop a tiered approach to data sovereignty, with strict localisation requirements for sensitive government and critical infrastructure data alongside more flexible mechanisms for commercial data transfers to key economic partners.

[80] Wawasan (n 25).

d) Explicitly incorporate relevant Islamic legal principles into the regulatory framework, particularly in defining privacy concepts, sensitive data categories, and data subject rights.[81] Brunei should consider incorporating Islamic Legal Principles into its data protection regime, as this would resonate with the country's cultural and legal traditions. Islamic teachings on confidentiality (star)[82] and the protection of personal dignity (*hurmah*) can serve as a normative foundation for the law, strengthening its legitimacy among Bruneians.[83] The Integration of these values could be particularly important in ensuring compliance with data protection laws in the private sector and among small and medium-sized enterprises, which may not be as familiar with Western data protection norms.

e) Implement a progressive compliance strategy that prioritises education and capacity-building over immediate enforcement, with implementation timelines tailored to organisational size and sector. To ensure smooth implementation, Brunei could adopt a phased regulatory approach, allowing for gradual expansion and refinement of data protection measures. For example:

- Initial focus on core privacy principles, such as consent, breach notification, and basic rights, with a clear roadmap for expansion to more complex issues such as cross-border data flows and sector-specific obligations.
- Sectoral regulations can be introduced later, particularly in sensitive sectors like healthcare, financial services, and e-commerce, where specific safeguards may be required.

---

[81] Malay (n 25).

[82] In the context of information security, 'star' likely refers to a classification level within a security model, particularly in government or organisations dealing with sensitive data. The 'strong star confidentiality rule' is a security model principle stating that access to information should be restricted based on a star-like hierarchy of secrecy levels, such as Top secret, confidential, etc. This ensures that individual can only access information at their own or a lower level of secrecy, preventing unauthorised disclosure.

[83] Kamali (n 74) 11-13.

This approach would also provide time to build institutional capacity within the Data Protection Authority and other relevant authorities.[84]

f) Establish a dedicated data protection authority with both regulatory and educational mandates, following Morocco's model of positioning the regulator as a partner in compliance rather than merely an enforcement entity.
g) Develop regional cooperation mechanisms, particularly within the ASEAN framework, to establish mutual recognition of data protection standards and facilitate responsible cross-border data flows. To further enhance Brunei's integration into the global digital economy, it should seek to establish international data adequacy agreement with key trading partners and regional blocs, such as the European Union, ASEAN, and the Gulf Cooperation Council (GCC).[85] Negotiating adequacy with the EU, for instance, would enable seamless data flows between Brunei and EU member states, boosting its attractiveness as a destination for international businesses and investments. This would also promote Brunei's alignment with global standards while providing legal certainty for cross-border data transfers.
h) Strengthening Public Awareness and Engagement: A key component of any successful data protection regime is public trust and engagement. There is also the need for Bruneians to understand the importance of the existence of such Data Protection Regulations. This could be achieved through the launching of a national public awareness campaign to: Inform citizens about their data privacy rights and responsibilities, educate businesses on compliance requirements and best practices in data handling, foster a culture of privacy and data stewardship, integrating these values into education and public discourse.

[84] Nout Wellink, 'Institutional Design and Regulatory Autonomy in Data Governance' (2023) 40 Regulatory Policy Journal 78.
[85] European Commission, 'Data Protection: Adequacy Decisions' (2024) <https://ec.europa.eu> accessed 25 April 2025.

i) Moreover, Brunei should avoid the negative experiences of most MENA countries but copy the likes of Morocco and the UAE to prioritise institutional independence and build the AITI's capacity as the DPA to manage both enforcement and public engagement. Public engagement and education, considering the phased implementation of data protection measures, will ensure that businesses and individuals utilise the available time to adapt to the new requirements and also play a pivotal role in fostering a privacy-conscious culture. As seen in the MENA region, effective data protection laws are not only about compliance but also about creating a shared understanding of privacy rights and responsibilities.

j) Lastly, Brunei must consider the international landscape, actively engaging in discussions on cross-border data flows and adequacy agreements. These steps will help Brunei integrate into the global digital economy, ensuring that its businesses can participate in international trade without facing data governance barriers. By learning from both MENA's successes and failures, Brunei can develop a data protection regime that is not only effective in protecting individual rights but also conducive to economic growth and technological innovation.