2025 Volume: 01 Issue: 07 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-38

CLOUD COMPUTING, DATA SOVEREIGNTY, AND REGULATORY GOVERNANCE IN GHANAS

Roland Yaw Kudozia*[1], Salifu Abdul-Razak[2], Evelyn Bediakoh-Adu[2]

[1]Gdirst Institute.

[2]National Communications Authority.

Article Received: 31 October 2025
Article Revised: 20 November 2025
Published on: 11 December 2025

***Corresponding Author: Roland Yaw Kudozia**
Gdirst Institute.

DOI: https://doi-doi.org/101555/ijrpa.3883

ABSTRACT

Cloud computing is gradually becoming central to Ghana's digitalisation agenda, underpinning initiatives in e-government, digital financial services and private-sector innovation. Decisions about where and how data are stored, processed and moved across borders are shaped by a complex legal and regulatory environment. This paper analyses Ghana's cloud-relevant legal framework, focusing on the Electronic Transactions Act, 2008 (Act 772), the Data Protection Act, 2012 (Act 843), the Cybersecurity Act, 2020 (Act 1038), and related sectoral instruments, together with emerging policy initiatives on data centres and cloud services. It situates Ghana's approach within wider African and global debates on data sovereignty, data localisation and cross-border data flows, drawing on continental frameworks such as the African Union's Digital Transformation Strategy for Africa and AU Data Policy Framework, as well as regional initiatives led by Smart Africa. Using a doctrinal and policy-analytic approach based entirely on secondary sources, the paper maps institutional mandates, identifies areas of overlap and fragmentation across key regulators, and examines the implications for cloud adoption by government, financial institutions and other organisations. It concludes by proposing options for a more coherent, risk-based cloud and data governance framework that can reconcile legitimate sovereignty and security concerns with the practical need for scalable, resilient cloud services in Ghana.

KEYWORDS: *Cloud computing; Data sovereignty; Data protection law; Regulatory governance; Ghana digital economy.*

INTRODUCTION

Cloud computing has become a foundational layer of contemporary information systems, enabling organisations to access scalable infrastructure, platforms and software services without commensurate investment in on-premises hardware. For countries pursuing ambitious digital transformation agendas, cloud services support the deployment of e-government platforms, the expansion of digital financial services and the modernisation of business processes across sectors. In Ghana, these dynamics intersect with a broader policy drive to build a robust digital economy, supported by national initiatives on connectivity, e-government and digital skills (Ministry of Communications and Digitalisation, 2023; World Bank Group, 2019, 2022).

At the same time, cloud computing raises sensitive questions about where data are stored, who controls them and which legal regime applies when data are processed across borders. Debates on "data sovereignty", data localisation and cross-border data flows have intensified globally in the wake of instruments such as the European Union's General Data Protection Regulation (GDPR) and landmark decisions on international data transfers, as well as in the context of national security and industrial-policy concerns. Across Africa, the African Union's Digital Transformation Strategy for Africa (2020–2030) and AU Data Policy Framework highlight the importance of secure, trusted and interoperable data ecosystems, while regional initiatives such as the Smart Africa Data Centre and Cloud Initiative seek to expand local hosting capacity and promote African-based cloud infrastructure (African Union Commission, 2020, 2022; Smart Africa, 2023).

Ghana sits at the intersection of these trends. The country has enacted a set of core digital-era statutes such as the Electronic Transactions Act, 2008 (Act 772), the Data Protection Act, 2012 (Act 843) and the Cybersecurity Act, 2020 (Act 1038) and has established specialised bodies including the Data Protection Commission, the Cyber Security Authority and the National Information Technology Agency. Sectoral regulators, notably the National Communications Authority and the Bank of Ghana, also exercise important functions in relation to infrastructure, service provision and outsourcing arrangements. These instruments and institutions together form the backbone of Ghana's legal environment for cloud computing and data processing.

However, they were not all designed with contemporary, hyperscale, cross-border cloud architectures in mind, and their interaction raises complex questions about data sovereignty, regulatory coordination and the compliance burden facing cloud users and providers.

Despite growing policy interest in cloud computing and the emergence of data-centre and cloud initiatives in Ghana, systematic academic analysis of the country's cloud-relevant legal and regulatory framework remains limited. Existing commentaries tend to focus either on data protection in general or on specific sectors such as banking and digital financial services, without providing a comprehensive mapping of cloud-related obligations, institutional mandates and cross-border data transfer regimes (e.g., Mensah, 2023; DLA Piper, 2024). This paper addresses that gap by offering a doctrinal and policy-analytic examination of how Ghana's laws and institutions govern cloud computing and data, and what this implies for cloud adoption and data sovereignty debates.

The paper is guided by three interrelated research questions:

1. How do Ghana's existing laws and regulations govern the storage, processing and cross-border transfer of data in cloud computing arrangements?
2. How are responsibilities for cloud-relevant issues—such as data protection, cybersecurity, critical information infrastructure and sector-specific oversight—distributed across Ghanaian institutions, and where do overlaps or gaps arise?
3. What are the implications of this legal and institutional configuration for data sovereignty, regulatory certainty and the practical adoption of cloud services by public- and private-sector actors in Ghana?

Using a structured review of statutes, policy documents, regulatory instruments and authoritative commentaries, the paper constructs an integrated view of Ghana's cloud-relevant regulatory environment. It situates the Ghanaian case within broader continental and global developments, and identifies specific areas where legal uncertainty, institutional fragmentation or misaligned incentives may increase compliance costs or slow cloud adoption. In doing so, the paper contributes to the emerging literature on cloud regulation and data governance in Africa and provides a reference point for policymakers, regulators, investors and service providers seeking to understand and improve Ghana's cloud governance landscape.

The remainder of the paper is structured as follows. Section 2 sets out the conceptual and normative background on cloud computing, data sovereignty and cross-border data governance. Section 3 examines Ghana's domestic legal framework, focusing on key statutes and sectoral instruments. Section 4 maps the institutional landscape and analyses potential fragmentation and overlap. Section 5 explores data sovereignty and cross-border data flows in practice, including the interaction with regional and continental frameworks. Section 6 discusses key challenges and risks for cloud adoption, and Section 7 proposes policy and regulatory recommendations. Section 8 concludes and outlines directions for future research.

2. Conceptual and normative background

Cloud computing is now widely recognised as a foundational element of contemporary information systems, enabling organisations to access computing, storage and software resources on demand over the internet rather than through on-premises infrastructure. In practice, cloud services are commonly grouped into infrastructure-, platform- and software-as-a-service models, with each model distributing technical and governance responsibilities differently between provider and customer. For many developing countries, cloud computing is seen as an opportunity to modernise public administration, deepen financial inclusion, and accelerate digital transformation, particularly when combined with investments in broadband networks and data-centre infrastructure (International Telecommunication Union, 2023; World Bank Group, 2019, 2023).

Two broad normative perspectives shape debates on cloud computing in Ghana and across Africa. The first is a rights-based data protection perspective, which emphasises the protection of individuals' personal data and privacy. This perspective is anchored in instruments such as the African Union Convention on Cyber Security and Personal Data Protection, the AU Data Policy Framework and, globally, the EU General Data Protection Regulation, all of which articulate core principles of lawfulness, fairness, purpose limitation, data minimisation, security and accountability, and address cross-border data transfers as a specific regulatory problem (African Union Commission, 2014, 2022; European Union, 2016). Ghana's Data Protection Act, 2012 (Act 843) reflects many of these principles and creates an independent Data Protection Commission with powers to supervise controllers and processors (Republic of Ghana, 2012; Mensah, 2023).

The second is a sovereignty and development perspective, which treats data as a strategic resource linked to national development, security and economic competitiveness. The African Union's Digital Transformation Strategy for Africa (2020–2030) and the AU Data Policy Framework both highlight the need to build trusted digital spaces, increase African control over data value chains and ensure that digital infrastructures, including data centres and cloud platforms, contribute to local and regional development (African Union Commission, 2020, 2022). These documents encourage member states to adopt robust data protection and cybersecurity regimes while also enabling cross-border data flows that support trade under the African Continental Free Trade Area and related initiatives.

Within this broader continental context, Ghana has articulated its own digital transformation ambitions through instruments such as the Ghana Digital Economy Policy and Strategy and sectoral strategies for digital financial services and e-government. These policies emphasise digital infrastructure, digital platforms, digital skills and an enabling regulatory environment as key pillars of economic transformation, and they explicitly reference cloud services and data centres as enablers of scalable, secure public and private digital services (Ministry of Communications and Digitalisation, 2023; World Bank Group, 2019, 2023).

The interaction between these normative strands, that is, individual rights, national sovereignty and development creates a complex landscape for cloud governance within which legal, regulatory and policy choices must be navigated (Mensah, 2023; African Union Commission, 2020, 2022; World Bank Group, 2019, 2023). Figure 1 summarises these normative pillars and situates Ghana's cloud and data governance at their intersection.

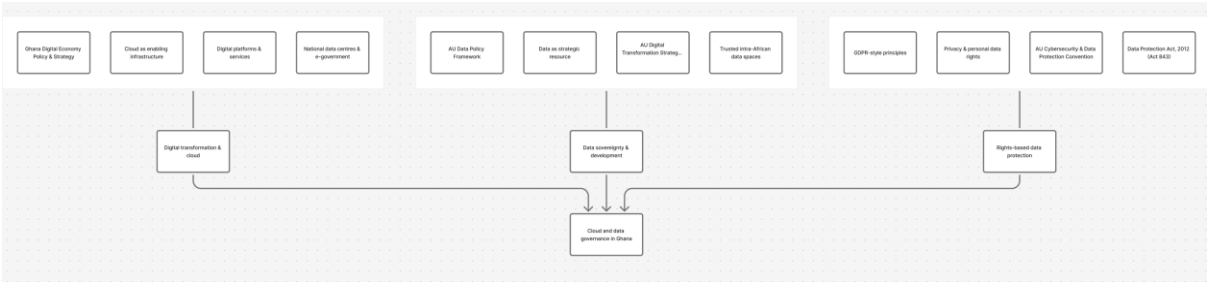

Figure 1: Normative pillars of cloud and data governance in Ghana.

Note. The Authors illustration of how three normative strands namely ights-based data protection, data sovereignty and development, and digital transformation and efficiency; these jointly shape debates on cloud and data governance in Ghana.

On the one hand, cloud computing promises efficiency, scalability and resilience; on the other, it raises concerns about jurisdiction, control over data, exposure to foreign legal orders and the concentration of technical and economic power in a small number of global providers. Ghana's legal and institutional framework sits at the intersection of these concerns. The remainder of the paper therefore examines how existing statutes, regulators and policies structure cloud-related decisions, how data sovereignty and cross-border data flows are managed in practice, and how a more coherent national cloud and data-centre governance framework might be developed to address identified gaps (Mensah, 2023; African Union Commission, 2020, 2022; World Bank Group, 2019, 2023).

3. Ghana's domestic legal framework for cloud and data governance

3.1 Electronic Transactions Act, 2008 (Act 772)

The Electronic Transactions Act, 2008 (Act 772) is one of Ghana's earliest foundational statutes for the digital environment. It provides legal recognition for electronic records and signatures, regulates the formation and validity of electronic contracts, and sets out obligations for service providers engaged in electronic commerce (Republic of Ghana, 2008). Although the Act predates mainstream public cloud adoption, it establishes several principles that remain relevant for cloud-based transactions, including provisions on the retention of electronic records, admissibility of electronic evidence, and liability of intermediaries and service providers.

For cloud computing, Act 772 is particularly important in clarifying that electronic records and signatures may not be denied legal effect solely because they are in electronic form, and that contracts formed by electronic means are valid and enforceable subject to general contract law (Republic of Ghana, 2008). This underpins the enforceability of cloud service agreements, service-level agreements and related digital contracts. However, the Act does not contain detailed, technology-specific rules on cloud infrastructure, data hosting or cross-border processing and therefore functions as a general legal backdrop rather than a sector-specific cloud regulation.

3.2 Data Protection Act, 2012 (Act 843)

The Data Protection Act, 2012 (Act 843) provides Ghana's core framework for the protection of personal data. It establishes the Data Protection Commission (DPC), sets out data protection principles and delineates the rights of data subjects and obligations of data

controllers and processors (Republic of Ghana, 2012). The Act applies to both public and private bodies that collect, hold, use or disclose personal data, and explicitly covers processing carried out by third parties on behalf of controllers, which is central to cloud computing arrangements.

Act 843 embodies familiar data protection principles lawfulness and fairness, purpose specification, compatibility of further processing, data minimisation, data quality, security safeguards and data subject participation that closely resemble those found in other data protection regimes. Controllers are required to register with the DPC, implement appropriate technical and organisational safeguards, and ensure that processors (including cloud service providers) provide sufficient guarantees regarding the security and confidentiality of personal data (Republic of Ghana, 2012; Mensah, 2023). In practice, this implies that Ghanaian organisations outsourcing processing to cloud providers must exercise due diligence, incorporate data protection clauses into contracts and monitor compliance.

of particular relevance to data sovereignty debates are the Act’s provisions on cross-border data transfers. The Act establishes control over international data flows primarily through its mandatory registration system for data controllers. Under Section 47(1)(g), a data controller must declare to the Data Protection Commission (DPC) "the name or description of the country to which the applicant may transfer the data." The DPC's power to grant (Section 49) or refuse registration (Section 48) based on whether sufficient safeguards for the data subject's privacy are in place effectively serves as the regulatory mechanism for authorizing transfers.

The Act’s framework for cross-border data control is further reinforced by principles that impose obligations related to foreign jurisdictions. For instance, Section 18(2) requires that when personal data originating from a foreign jurisdiction is sent to Ghana for processing, it must be processed in compliance with the data protection legislation of that foreign jurisdiction. Furthermore, Section 29(4) states that where a data processor is not domiciled in Ghana, the data controller must ensure the processor complies with Ghana’s relevant laws.

Although the Act does not adopt a formal adequacy decision regime like the EU's GDPR, it clearly introduces a conditional, authorization-based approach to international data transfers. This framework must be taken into account when Ghanaian organisations use cloud services hosted in foreign jurisdictions, as the legality of such transfers is contingent on registration

disclosure and the DPC's oversight of the provided safeguards (Mensah, 2023; DLA Piper, 2024).

3.3 Cybersecurity Act, 2020 (Act 1038)

The Cybersecurity Act, 2020 (Act 1038) creates a comprehensive institutional and regulatory framework for cybersecurity in Ghana, including the designation and protection of critical information infrastructure (CII), the regulation of cybersecurity service providers, and the establishment of the Cyber Security Authority (Republic of Ghana, 2020). Section 39 of the Cybersecurity Act, 2020 (Act places obligations on owners of CII to implement cybersecurity measures, report incidents and cooperate with the Authority, and provides for the development of national cybersecurity standards and guidelines.

Although Act 1038 does not use the term "cloud computing" extensively, many cloud-based systems in sectors such as banking, telecommunications, government and energy can fall within the definition of CII where their compromise would have a debilitating impact on national security, the economy, public health or safety. In such cases, cloud infrastructure and services used to support critical systems are subject to heightened cybersecurity requirements and oversight. The Act also provides for the accreditation of cybersecurity professionals and service providers, which can intersect with cloud security auditing and incident response arrangements (Republic of Ghana, 2020; Cyber Security Authority, n.d.).

Importantly, the Cybersecurity Act interacts with the Data Protection Act and sectoral regulations by introducing an integrated approach to incident reporting and resilience. For organisations using cloud services to host or process critical data, this means that contractual arrangements with cloud providers must take into account not only data protection obligations but also cybersecurity controls, incident notification timelines and cooperation duties vis-à-vis the Cyber Security Authority. Where cloud infrastructure is located outside Ghana, questions arise as to how national incident reporting and enforcement powers operate in practice, adding another layer of complexity to data sovereignty considerations.

3.4 Sectoral regulations and soft-law instruments

Beyond horizontal statutes, several sectoral regulators in Ghana have issued instruments that have a direct or indirect bearing on cloud computing, data centres and outsourcing. Two are particularly notable for this analysis: the Bank of Ghana in relation to financial services, and

the National Communications Authority and National Information Technology Agency in relation to telecommunications, data centres and government ICT.

The Bank of Ghana has issued guidelines and directives that address the use of third-party service providers, outsourcing and information security for regulated financial institutions (Bank of Ghana, 2024. These instruments require banks and specialised deposit-taking institutions to conduct due diligence on service providers, maintain oversight of outsourced functions, ensure that outsourcing contracts contain appropriate confidentiality and security provisions, and obtain the Bank's approval for certain high-risk outsourcing arrangements (Bank of Ghana, 2024). While these guidelines do not always name "cloud computing" explicitly, cloud-based services fall squarely within the scope of outsourcing where critical systems or customer data are hosted on third-party infrastructure. For cross-border cloud arrangements, institutions must demonstrate that data protection, business continuity and regulatory access requirements are satisfied.

On the infrastructure side, the National Communications Authority (NCA) and the National Information Technology Agency (NITA) play important roles. The NCA regulates electronic communications networks and services, including data and internet service providers, and has been involved in licensing and oversight of submarine cable landings and data connectivity infrastructure (National Communications Authority, 2017, 2024). NITA, as the government's ICT technical arm, is responsible for national IT standards, government networks and data-centre projects, including the national data centre that underpins aspects of e-government. Recent NITA-led processes, supported by Smart Africa, aim to develop a Regulatory Framework for Data Centres in Ghana, which will set out requirements for design, operation, resilience and security of data-centre facilities (National Information Technology Agency, 2023; Regulatory Framework for Data Centres, n.d.; Smart Africa, 2023).

In addition, Ghana's Digital Economy Policy and Strategy articulates a policy commitment to promote secure, resilient cloud and data-centre infrastructure, government cloud services and digital public platforms, although it is primarily a strategy rather than a binding legal instrument (Ministry of Communications and Digitalisation, 2023). Together, these sectoral and policy instruments supplement Acts 772, 843 and 1038 by providing more specific expectations for certain industries and by signalling the government's intention to position Ghana as a regional data and cloud hub. However, they also contribute to a landscape in

which responsibilities and rules are distributed across multiple institutions, setting the stage for potential overlaps and inconsistencies that are explored in subsequent sections.

These horizontal statutes and sectoral instruments establish the core legal architecture for cloud and data governance in Ghana, even though they were not all designed with contemporary hyperscale cloud models in mind (Republic of Ghana, 2008, 2012, 2020; Ministry of Communications and Digitalisation, 2023). Figure 2 provides a consolidated overview of this domestic framework and its main institutional linkages.

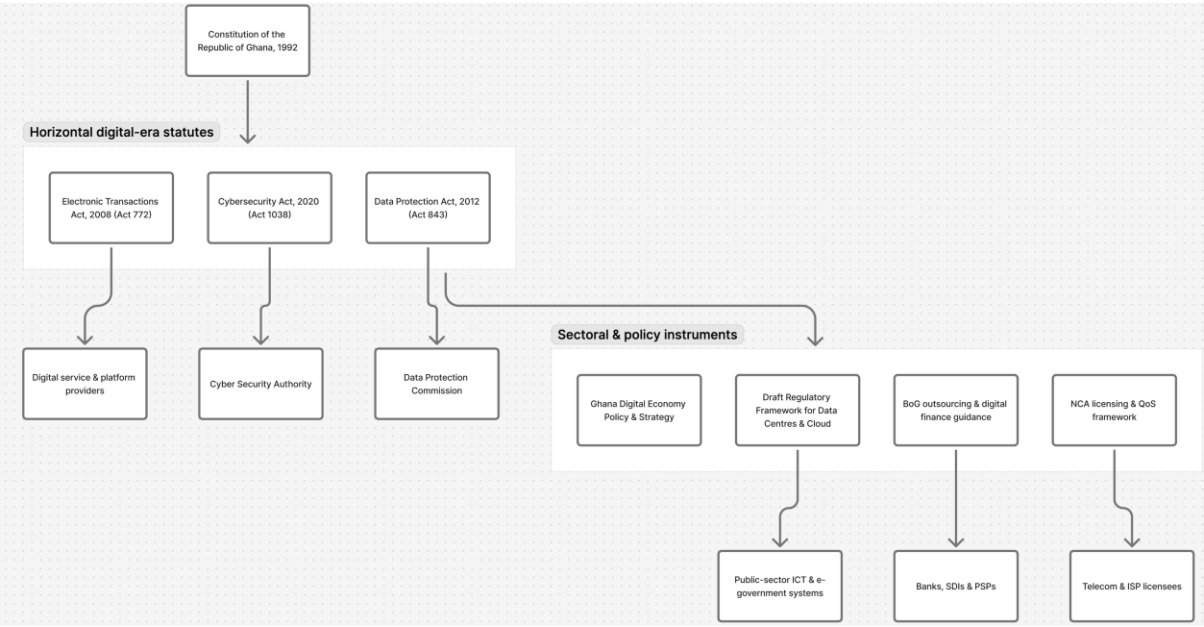

Figure 2 : Domestic legal and regulatory framework for cloud and data governance in Ghana.

Note. Authors' depiction of the core legal instruments namely Constitution, Electronic Transactions Act, Data Protection Act, Cybersecurity Act and key sectoral and policy instruments, together with their links to principal authorities such as the DPC, CSA, NCA, NITA and Bank of Ghana.

4. Institutional landscape and regulatory fragmentation

Ghana's cloud computing and data-governance environment is shaped by a relatively dense constellation of public institutions whose mandates partially overlap. At the apex, the Ministry of Communications,Digital Innovation and Technology is responsible for overall sector policy, including the Ghana Digital Economy Policy and Strategy and related initiatives on e-government, data centres and emerging technologies (Ministry of

Communications and Digitalisation, 2023). Beneath this policy layer, a number of specialised regulators and authorities exercise statutory powers over communications infrastructure, data protection, cybersecurity and financial services, all of which directly affect cloud deployment.

The National Communications Authority (NCA) is the central regulator for electronic communications networks and services. Established under the National Communications Authority Act, 2008 (Act 769) the NCA licenses and regulates telecommunications operators, internet service providers and other communications service providers, manages spectrum and numbering resources and enforces quality-of-service and consumer-protection standards (Republic of Ghana, 2008; World Bank Group, 2019). These functions extend to submarine cable operators, wholesale carriers and data providers, placing the NCA at the core of decisions that determine connectivity for cloud services.

The National Information Technology Agency (NITA) operates as the government's ICT implementation and standards body. Under its establishing legislation(National Information Technology Agency Act, 2008 (Act 771) and associated policy instruments, NITA is responsible for regulating ICT within the public sector, managing core e-government platforms such as the government network (GOVNET) and the national data centre, and developing technical standards and guidelines for public information systems (National Information Technology Agency, 2023; Ministry of Communications and Digitalisation, 2023). Recent initiatives to develop a national data-centre and cloud regulatory framework with support from Smart Africa signal an intention to give NITA a more explicit role in cloud and data-centre governance.

The Data Protection Commission (DPC) is the statutory authority created under the Data Protection Act, 2012 (Act 843). The Act sets out substantive data-protection principles, establishes a registration regime for data controllers and processors and grants the Commission powers to investigate complaints, conduct compliance checks and issue guidance (Republic of Ghana, 2012). Legal analysis of Act 843 emphasises that organisations remain responsible for compliance when they outsource processing to cloud providers and that cross-border transfers of personal data are subject to the Act's general provisions on lawful processing, security safeguards and accountability, even in the absence of detailed transfer rules (Mensah, 2023; DLA Piper, 2024).

The Cyber Security Authority (CSA), created under the Cybersecurity Act, 2020 (Act 1038), oversees the protection of critical information infrastructure, licensing of cybersecurity service providers and coordination of incident response. Telecommunications networks, financial systems and key public-sector platforms can be designated as critical information infrastructure, bringing many cloud-reliant systems within the CSA's remit (Republic of Ghana, 2020). In parallel, the Bank of Ghana supervises banks, specialised deposit-taking institutions and regulated payment service providers, including their use of outsourced and cloud-based solutions for core and ancillary services, and expects institutions to retain effective oversight over such arrangements (Pazarbasioglu et al., 2020; Senyo et al., 2022).

In principle, these institutions are complementary: the NCA focuses on networks and services, NITA on public ICT infrastructure and standards, the DPC on personal-data protection, the CSA on cybersecurity and critical information infrastructure, and the Bank of Ghana on financial stability and consumer protection in the financial sector. In practice, however, commentators point to areas of overlap, especially in relation to data security, incident reporting and cross-border data governance (Mensah, 2023; World Bank Group, 2019, 2023). For example, a cloud-based financial platform may simultaneously fall under the DPC for data protection, the CSA for cybersecurity, the NCA for communications-service regulation, NITA for government ICT standards if it interfaces with public systems and the Bank of Ghana for financial supervision.

This configuration can create what might be termed a "many doors" problem for cloud providers and institutional users who must engage multiple authorities for interrelated issues of data protection, cybersecurity, infrastructure and sectoral risk (Mensah, 2023; World Bank Group, 2019, 2023). Figure 3 depicts this institutional landscape and highlights the main areas of overlapping responsibility. Decisions about how and where data may be hosted, which incidents must be reported to which authority and how to design outsourcing contracts that satisfy multiple regulatory expectations may be subject to overlapping and sometimes incomplete guidance. Empirical work on cloud adoption in Ghana suggests that institutional pressures and perceived regulatory complexity influence adoption decisions alongside technical and organisational factors (Adjei et al., 2021; Coffie et al., 2021). At the continental level, the AU Data Policy Framework underscores the importance of coherent, well-coordinated institutional architectures for data governance and cautions against fragmented

regulatory regimes that increase uncertainty and compliance costs (African Union Commission, 2022).

Overall, Ghana's institutional landscape provides a strong foundation in terms of specialised bodies and formal mandates, but the distribution of roles and the level of coordination are still evolving. Planned reforms to communications and ICT legislation and ongoing work on data-centre and cloud frameworks offer opportunities to clarify lead-agency responsibilities and streamline regulatory interfaces. The proposed national cloud and data-centre governance framework in later sections builds on this observation by suggesting a more structured allocation of functions among existing institutions rather than the creation of entirely new agencies.

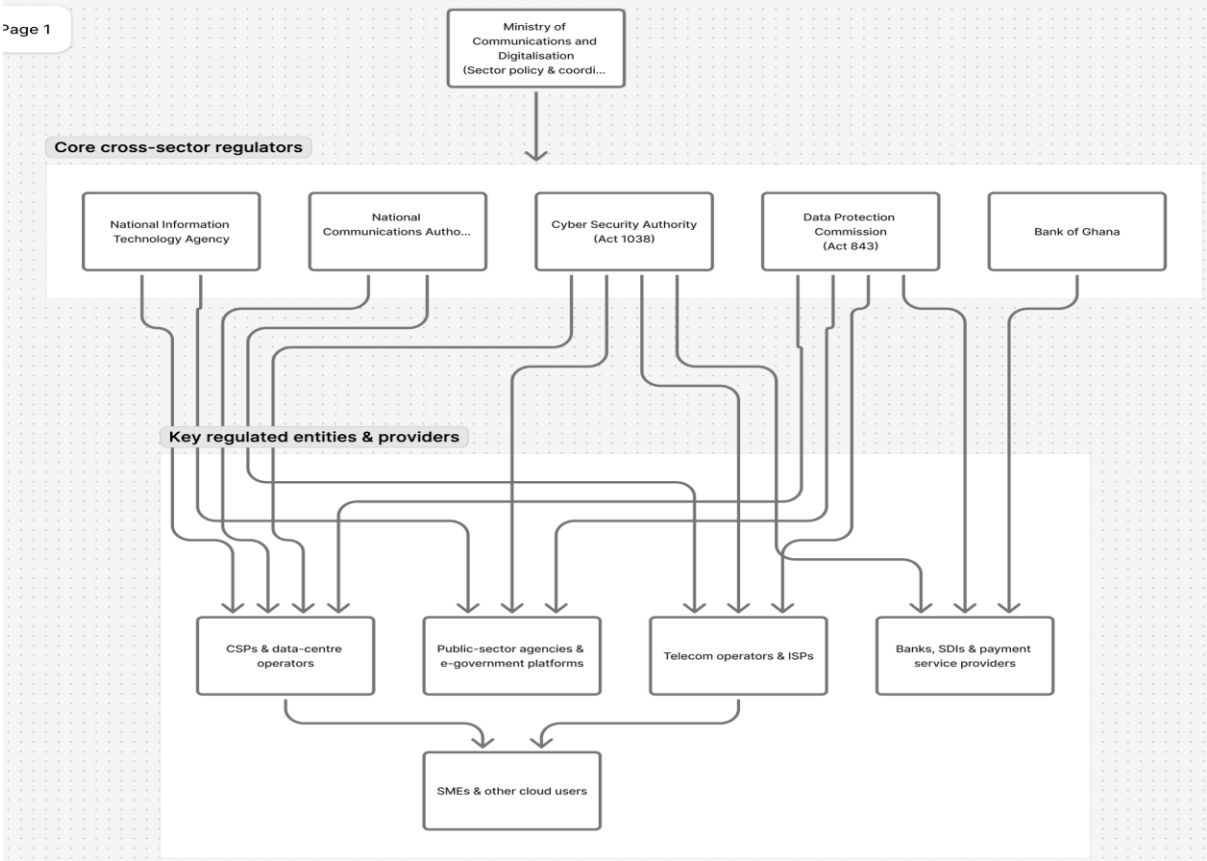

Figure 3 Institutional landscape for cloud and data governance in Ghana

Note. Authors illuation shows the Ministry of Communications,Digital Innovation and Technology at the policy apex, the core cross-sector regulators (DPC, CSA, NCA, NITA, Bank of Ghana) in the middle layer, and key regulated entities and cloud/data-centre users

(public agencies, telcos, financial institutions, CSPs, SMEs) at the base, with indicative overlapping relationships.

5. Data sovereignty and cross-border data flows in practice

Debates on data sovereignty in Ghana are most visible in the rules and practices governing cross-border data transfers, particularly in the context of cloud computing. The Data Protection Act, 2012 (Act 843) does not contain a discrete chapter on international data transfers comparable to the GDPR, but it defines processing broadly to include disclosure and transmission of personal data, and applies its general principles of lawfulness, security and accountability to all processing activities, whether domestic or cross-border (Republic of Ghana, 2012; Mensah, 2023). In legal commentary, this has been interpreted to mean that controllers remain fully responsible for compliance when data are processed in foreign or regional data centres and must ensure that contracts and technical measures provide safeguards equivalent to those required by the Act (Mensah, 2023; DLA Piper, 2024).

In practice, there is evidence that some controllers intending to transfer data outside Ghana informally seek guidance or comfort from the Data Protection Commission, for example through correspondence outlining the nature and purpose of the transfer and the protections in place. However, the criteria used to assess such transfers and the processes followed are not yet codified in detailed regulations or guidelines. This contrasts with the more structured mechanisms envisaged in instruments such as the AU Data Policy Framework, which encourages member states to define conditions for trusted cross-border data flows, including adequacy assessments, standard contractual clauses and other transfer tools (African Union Commission, 2022). The result is a degree of legal uncertainty for complex cloud arrangements involving multiple jurisdictions and sub-processors.

Sectoral practice further shapes how cross-border data governance plays out. In the financial sector, regulated institutions are expected to maintain effective oversight and control over outsourced and cloud-based services, ensuring that confidentiality, security and regulatory access are not compromised when data are processed outside Ghana (Pazarbasioglu et al., 2020; Senyo et al., 2022). For mission-critical systems, some institutions have opted for hybrid architectures that combine local or regional hosting for core workloads with global cloud services for analytics, testing or non-critical applications. Similar dynamics are evident in the public sector, where efforts to consolidate e-government platforms in national data

centres coexist with selective use of commercial cloud services for specific applications and back-up arrangements (National Information Technology Agency, 2023; Ministry of Communications and Digitalisation, 2023).

These patterns reflect a wider continental tension between aspirations for greater data sovereignty and the practical realities of infrastructure and market development. The AU Digital Transformation Strategy and Data Policy Framework both emphasise the importance of treating data as a strategic resource and of building African capacity in data-centre and cloud infrastructure, while at the same time promoting intra-African data flows and participation in the global digital economy (African Union Commission, 2020, 2022). Analyses of Africa's data-centre landscape show, however, that multi-tenant, carrier-neutral data-centre capacity remains concentrated in a small number of countries, and that many states rely on regional hubs and global cloud regions for advanced services (Africa Data Centres Association, 2023; Africa Data Centres Association & Oxford Business Group, 2024).

For Ghana, this means that a rigid or hastily implemented localisation agenda could have unintended consequences. Overly broad residency requirements, introduced without sufficient domestic or regional capacity, may lead to higher costs, reduced resilience and limited access to advanced cloud services, particularly for smaller organisations. Conversely, a lack of clear rules on cross-border transfers, data classification and sovereignty safeguards can undermine trust, weaken bargaining power with large providers and limit Ghana's ability to align with emerging African data-governance frameworks and digital trade arrangements (African Union Commission, 2022; World Bank Group, 2023; World Trade Organization, 2024).

The analysis in this paper suggests that Ghana currently occupies a middle position. It has enacted a data-protection statute, established dedicated authorities for data protection and cybersecurity, and is actively seeking to expand its data-centre and cloud ecosystem through national and regional initiatives (Republic of Ghana, 2012, 2020; Smart Africa, 2022a, 2022b; National Information Technology Agency, 2023). At the same time, the absence of explicit transfer mechanisms, the fragmentation of institutional responsibilities and the reliance on informal practices for some cross-border decisions indicate that the country's data-sovereignty regime is still under construction.

The proposed risk-based localisation and data-sovereignty measures, and the indices for workload risk, sovereignty assurance and organisational compliance outlined in later sections, are intended to provide practical tools for navigating this transitional phase. They offer a way to differentiate between categories of data and workloads, calibrate hosting and transfer conditions to risk, and strengthen self-governance within organisations, while Ghana continues to refine its statutory and regulatory instruments in line with continental guidance and domestic priorities (African Union Commission, 2022; Mensah, 2023; World Bank Group, 2023).

6. Key challenges and risks for cloud adoption

The preceding sections show that Ghana has put in place a substantive body of digital-era law and a relatively dense institutional architecture for ICT, data protection and cybersecurity. However, the way these elements operate in practice generate several challenges and risks for cloud adoption. Many of these are consistent with broader patterns observed in African digital transformation, but they also reflect specific features of Ghana's legal and institutional context (African Union Commission, 2020, 2022; World Bank, 2023).

6.1 Regulatory uncertainty and overlapping mandates

A first challenge is regulatory uncertainty arising from overlapping mandates and the absence of detailed cloud-specific guidance. As earlier sections highlighted, cloud-relevant issues such as data protection, cybersecurity, critical information infrastructure, outsourcing and sectoral supervision are divided among the Data Protection Commission, the Cyber Security Authority, the National Communications Authority, the National Information Technology Agency and the Bank of Ghana.

Mensah's doctrinal analysis of Ghana's Data Protection Act underscores that, while Act 843 provides a broadly adequate framework for personal data protection, it does not contain a structured mechanism for assessing the adequacy of foreign data-protection regimes or a detailed architecture for cross-border transfers (Mensah, 2023). In practice, some controllers seek guidance from the Data Protection Commission on a case-by-case basis when they intend to transfer data abroad, but the criteria and processes for such assessments are not transparently codified. This implies that, for cloud arrangements involving foreign data centres, organisations may be uncertain about the precise conditions under which cross-border processing is acceptable.

At continental level, the African Union's Digital Transformation Strategy and AU Data Policy Framework both call for coherent, predictable data-governance regimes that facilitate trusted cross-border data flows while safeguarding fundamental rights and national interests (African Union Commission, 2020, 2022). The contrast between these aspirations and the relatively implicit cross-border rules in Act 843 contributes to an environment in which cloud providers and institutional users face multiple points of contact and interpretive uncertainty. For smaller organisations with limited legal and compliance capacity, this uncertainty can become a practical barrier to undertaking ambitious cloud migrations, even where the underlying laws are not explicitly restrictive.

6.2 Enforcement, compliance and capacity gaps

A second challenge concerns the gap between formal legal provisions and effective enforcement. Mensah (2023) notes that, more than a decade after the adoption of Act 843, compliance with registration and data-protection obligations remains uneven in Ghana, particularly among smaller enterprises and public bodies. Limited financial and technical resources at the Data Protection Commission constrain its ability to audit controllers systematically and to provide detailed, sector-specific guidance on complex arrangements such as multi-tenant cloud services (Mensah, 2023).

Similar capacity issues are visible in wider analyses of Africa's digital transformation. The World Bank's *Digital Africa* report points to institutional capacity and regulatory capability as critical determinants of whether countries can translate digital policies into effective practice, particularly in areas such as data governance, cybersecurity and digital platforms (World Bank, 2023). Where regulators are under-resourced, organisations may perceive the risk of non-compliance as low, which can weaken incentives to invest in robust data-protection and cloud-security governance. At the same time, insufficient enforcement can undermine citizens' trust in digital systems and make it harder for governments to demonstrate that their frameworks meet international expectations for adequacy and interoperability.

In the specific context of cloud computing, this enforcement gap complicates the shared responsibility model under which controllers must exercise due diligence over cloud providers and ensure that appropriate contractual and technical safeguards are in place. Without consistent supervisory practice and clear interpretive guidance, particularly in

relation to cross-border arrangements, controllers may be unsure how regulators will assess compliance, and cloud providers may struggle to align their standardised global offerings with Ghana-specific expectations.

6.3 Skills, organisational capacity and cost-related risks

A third cluster of challenges relates to skills and organisational capacity, which have been widely identified as constraints on digital transformation and cloud adoption across Africa. The International Finance Corporation's study on digital skills in Sub-Saharan Africa, with a spotlight on Ghana, finds that digital skills shortages are pervasive and affect both basic ICT use and more advanced capabilities needed for developing and managing digital systems (International Finance Corporation, 2019). The World Bank similarly highlights that African economies face significant gaps in advanced digital skills required for cloud computing, cybersecurity, data analytics and platform development, even as demand for such skills grows rapidly (World Bank, 2023).

For Ghanaian organisations, these constraints are especially acute in sectors that would benefit most from cloud-enabled transformation, such as public administration, small and medium-sized enterprises and smaller financial institutions. Adjei et al. (2021) show that institutional and organisational factors including internal capabilities, top management support and perceived regulatory pressures play an important role in shaping cloud computing adoption in Ghanaian firms. Their findings suggest that, even where infrastructure and basic awareness exist, limited internal capacity can delay or constrain adoption (Adjei et al., 2021).

Cloud migration also introduces new cost structures and risk profiles. While cloud services can reduce up-front capital expenditure on hardware, they shift costs toward recurring operating expenditure and require careful management of service selection, usage patterns and contractual terms. In environments where financial planning capacity is limited and cloud pricing models are not well understood, there is a risk of cost overruns, inefficient use of resources or dependency on a single provider. Combined with the skills shortages noted above, this can lead organisations to favour incremental, cautious deployments rather than fully leveraging the elasticity and scalability that cloud platforms can offer.

6.4 Data sovereignty, localisation pressures and regional competitiveness

A final set of challenges concerns how Ghana navigates data sovereignty and localisation pressures while remaining competitive as a destination for digital and cloud investment. The AU Data Policy Framework emphasises the need for African states to treat data as a strategic resource, develop trusted data spaces, and support intra-African data flows consistent with the African Continental Free Trade Area (African Union Commission, 2022). This continental agenda encourages stronger domestic data-protection and cybersecurity regimes and, in some cases, differentiated approaches to the handling of sensitive or strategic datasets.

At the same time, African data-centre capacity remains relatively limited compared with global regions. Analyses by the Africa Data Centres Association and Oxford Business Group highlight that Africa still accounts for a small share of the world's multi-tenant data-centre footprint, with a handful of countries hosting the majority of carrier-neutral capacity (Africa Data Centres Association & Oxford Business Group, 2024). For Ghana, this creates a tension between aspirations to keep more data within national or regional jurisdictional control and the practical reliance on regional or global cloud regions for certain services.

If localisation pressures are expressed through fragmented, overlapping or informally communicated expectations rather than clear, risk-based rules, they can produce unintended consequences: higher costs for organisations constrained to use scarce local infrastructure; reduced resilience where local facilities lack redundancy; and a perception among investors and cloud providers that the regulatory environment is unpredictable relative to competing hubs in the region. Conversely, failing to clarify sovereignty and transfer rules may leave sensitive data exposed to legal and security uncertainties and limit Ghana's ability to align with emerging African data-governance frameworks.

In this context, the main challenge is not whether Ghana should pursue data sovereignty, an objective shared across continental policy documents but how it does so. The analysis in this section suggests that Ghana will need to refine and formalise its cross-border data-transfer rules, clarify institutional roles and develop risk-based guidance that distinguishes between categories of data and workloads. Doing so would help reconcile legitimate sovereignty and security aims with the practical demands of scalable, interoperable cloud services and strengthen Ghana's position within evolving regional data and cloud ecosystems (African

Union Commission, 2020, 2022; World Bank, 2023). Figure 4 summarises the main clusters of challenges identified in this section and their interrelationships.

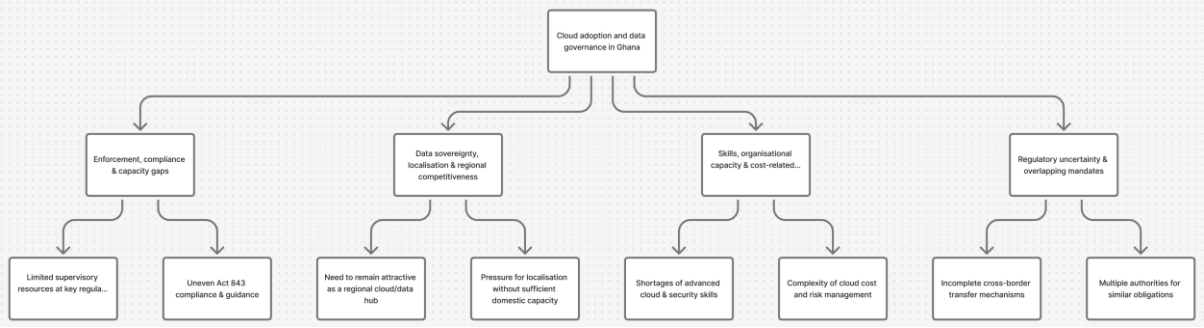

Figure 4 Main challenge clusters for cloud adoption and data governance in Ghana.

Note. The figure groups the analysis into four interrelated clusters: (1) regulatory uncertainty and overlapping mandates; (2) enforcement, compliance and capacity gaps; (3) skills, organisational capacity and cost-related risks; and (4) data sovereignty, localisation pressures and regional competitiveness.

7. Policy and regulatory recommendations

The analysis suggests that Ghana has already laid important foundations for cloud computing through its general digital legislation, emerging data-centre initiatives and digital economy strategies. At the same time, gaps in cross-border data-transfer rules, overlapping institutional mandates, limited enforcement capacity and skills constraints pose significant challenges for cloud adoption and data sovereignty. This section sets out broad policy and regulatory directions to address these challenges. The subsequent section (Section 8) then translates these directions into a more concrete proposed national cloud and data-centre governance framework for Ghana, offering a structured model that could guide future regulations and institutional reforms.

7.1 Clarifying cross-border data-transfer rules and tools

A first priority is to clarify and operationalise rules for cross-border data transfers under the Data Protection Act, 2012 (Act 843). Mensah's analysis shows that while Act 843 establishes robust general principles for personal data protection, it does not provide detailed mechanisms for assessing the adequacy of foreign regimes or for structuring international transfers (Mensah, 2023). The Data Protection Commission could address this by issuing guidance that:

1. sets out criteria for determining when a destination jurisdiction offers "adequate" protection, drawing on the AU Data Policy Framework and comparative practice;
2. recognises specific transfer tools such as standard contractual clauses, data-processing agreements and binding intra-group policies, and provides model clauses adapted to Ghanaian law; and
3. clarifies expectations for due diligence and documentation when controllers engage cloud providers that process data in multiple jurisdictions.

   Section 8 incorporates these directions by proposing that cross-border transfer tools and adequacy criteria form a dedicated component of the national cloud and data-centre governance framework, anchored in Act 843 and aligned with African Union data-governance principles (African Union Commission, 2022).

7.2 Strengthening institutional coordination and lead-agency roles

Given the number of bodies with cloud-relevant mandates, a second recommendation is to formalise coordination mechanisms and designate lead roles for specific risk domains. Under the policy authority of the Ministry of Communications and Digitalisation, Ghana could establish an inter-agency "cloud and data governance coordination mechanism" that brings together the Data Protection Commission, Cyber Security Authority, National Communications Authority, National Information Technology Agency and Bank of Ghana.

This mechanism could adopt a memorandum of understanding or framework agreement that:

1. allocates lead responsibility for personal-data protection and cross-border transfers to the Data Protection Commission;
2. recognises the Cyber Security Authority as the lead on cybersecurity standards and incident response, particularly for critical information infrastructure;
3. clarifies the NCA's role in relation to infrastructure and network-service regulation;
4. specifies NITA's responsibilities for government cloud, national data centres and ICT standards in the public sector; and
5. sets out how sectoral regulators such as the Bank of Ghana coordinate with horizontal regulators when supervising cloud-dependent institutions.

Section 8 develops this idea further by embedding these lead-agency roles into the proposed governance architecture of the national framework, so that institutional coordination is not ad hoc but part of a clearly articulated design (Mensah, 2023; Ministry of Communications and Digitalisation, 2023; World Bank, 2023).

7.3 Developing a national cloud and data-centre governance framework

A third recommendation which central to the contribution of this paper is for Ghana to consolidate existing instruments into a national cloud and data-centre governance framework. Rather than treating cloud and data centres solely through dispersed statutes and sectoral rules, Ghana could adopt an integrated framework that:

1. defines core objectives for cloud and data-centre governance;
2. articulates roles and responsibilities of key institutions;
3. links categories of data and workloads to appropriate hosting and transfer conditions; and
4. sets baseline requirements for cloud and data-centre providers.

Section 8 elaborates this proposal as a concrete, Ghana-specific framework. It sets out the objectives and scope of such a framework, describes a governance architecture with clear lead-agency roles, proposes a structured classification of data and workloads, and sketches baseline requirements for providers and mechanisms for compliance and coordination. In doing so, it moves beyond high-level recommendations to offer a practical template that policymakers and regulators could adapt and refine (African Union Commission, 2020, 2022; Africa Data Centres Association & Oxford Business Group, 2024; World Bank, 2023).

7.4 Adopting risk-based localisation and sovereignty measures

Rather than pursuing broad, undifferentiated localisation requirements, Ghana should adopt a risk-based approach to data sovereignty that distinguishes clearly between data categories. The AU Data Policy Framework encourages member states to promote trusted cross-border data flows while protecting categories of data that are strategic or sensitive (African Union Commission, 2022). For Ghana, this suggests carefully targeted localisation or regionalisation measures, for example applying stricter residency or mirroring requirements to critical government data, key financial-system data and specially classified national security information.

For other types of data, particularly routine business workloads, the emphasis could be placed on ensuring that cloud providers meet appropriate data-protection and cybersecurity standards irrespective of location, rather than on imposing absolute residency requirements. Section 8 operationalises this recommendation through a proposed data and workload classification scheme, which calibrates hosting and transfer conditions to risk levels and helps reconcile

sovereignty concerns with the need for scalable, resilient cloud services (Africa Data Centres Association & Oxford Business Group, 2024; World Bank, 2023).

7.5 Enhancing regulatory capacity, guidance and support

Effective cloud governance depends not only on the content of rules but also on regulatory capacity and guidance. Building on existing reforms, Ghana could invest in specialised cloud and data-governance expertise within the Data Protection Commission, Cyber Security Authority, NCA, NITA and sectoral regulators. This might include dedicated units responsible for issuing sector-specific cloud guidelines, analysing emerging service models and engaging with industry and civil society.

Given the digital-skills gaps highlighted by studies of Ghana and the wider region (International Finance Corporation, 2019; World Bank, 2023), regulators could also play a stronger role in capacity-building for cloud adoption. This could involve publishing templates for cloud contracts and data-processing agreements, organising workshops for public-sector and SME decision-makers, and collaborating with universities and professional bodies on cloud and data-governance training. Section 8 assumes such capacity-building as a necessary implementation pillar of the proposed framework and links it to the organisational and institutional factors that empirical work identifies as important for cloud adoption in Ghana (Adjei et al., 2021).

7.6 Measuring progress and fostering stakeholder dialogue

Finally, Ghana would benefit from systematic measurement and stakeholder dialogue around cloud and data governance. In line with the AU Data Policy Framework's emphasis on evidence-based policymaking (African Union Commission, 2022), the government could develop a cloud and data-governance scorecard that tracks progress on regulatory clarity, institutional coordination, infrastructure and enforcement. Regular publication of such a scorecard, combined with structured consultations involving cloud providers, telecommunications operators, financial institutions, SMEs, civil society and academia, would help identify emerging issues early and adjust regulatory approaches as needed.

Section 8 incorporates this idea by proposing that monitoring and stakeholder engagement be embedded in the implementation and phasing of the national framework, rather than treated as a separate, optional activity. This would support iterative refinement of rules, maintain alignment with continental initiatives and enhance Ghana's credibility as a proactive,

predictable jurisdiction for cloud and data-centre investment (African Union Commission, 2020, 2022; World Bank, 2023).

These recommendations taken together, in this section set the strategic direction for reform, while the subsequent section translates that direction into a more detailed national cloud and data-centre governance framework that can serve as a concrete reference point for policymakers and regulators.

8. Proposed national cloud and data-centre governance framework for Ghana

This section outlines a proposed national cloud and data-centre governance framework for Ghana, building directly on the legal and institutional analysis presented in earlier sections and on the policy directions articulated in the Ghana Digital Economy Policy and Strategy, the African Union's Digital Transformation Strategy for Africa and the AU Data Policy Framework (African Union Commission, 2020, 2022; Ministry of Communications and Digitalisation, 2023). The objective is not to prescribe a detailed legal instrument, but rather to articulate a coherent structure that can guide future regulations, policy guidelines and institutional arrangements.

8.1 Objectives and scope

The overarching objective of the proposed framework is to provide a clear, risk-based and nationally coherent foundation for the governance of cloud services and data-centre infrastructure in Ghana. The framework is intended to support four interrelated aims. First, it should enhance the security, resilience and trustworthiness of cloud and data-centre services used by public institutions, financial entities, critical infrastructure operators and private enterprises. Second, it should clarify data-sovereignty and cross-border data-transfer conditions in a way that aligns with Act 843 and emerging African norms, thereby reducing legal uncertainty for controllers and processors. Third, it should promote the development of competitive, carrier-neutral, multi-tenant data-centre and cloud markets in Ghana, consistent with regional initiatives to increase Africa's data-centre footprint (Africa Data Centres Association & Oxford Business Group, 2024; African Union Commission, 2022). Finally, it should streamline institutional roles so that regulators and supervisory bodies can implement their mandates in a coordinated, efficient manner.

In terms of scope, the framework is intended to cover both cloud service provision (including infrastructure-, platform- and software-as-a-service, and related managed services) and data-

centre facilities used to host such services, whether operated by public entities, licensed communications providers or independent commercial operators. It encompasses domestic providers operating within Ghana and foreign providers offering services to Ghanaian controllers and data subjects, to the extent that Ghanaian law applies.

8.2 Governance architecture

The governance architecture envisaged by the framework rests on a clear hierarchy of instruments and roles. At the policy apex, the Ministry of Communications and Digitalisation would retain responsibility for overall cloud and data-centre policy, including alignment with national development strategies and continental frameworks (Ministry of Communications and Digitalisation, 2023; African Union Commission, 2020, 2022). Beneath this, the framework would formally designate lead agencies for specific functional domains. The governance architecture envisaged by the framework rests on a clear hierarchy of instruments and roles, with the Ministry of Communications and Digitalisation at the policy apex and designated lead agencies for personal data protection, cybersecurity, communications infrastructure, public-sector ICT and financial stability (African Union Commission, 2020, 2022; Ministry of Communications and Digitalisation, 2023; World Bank Group, 2019, 2023). Figure 5 presents this proposed governance architecture and the relationships between the core institutions and cloud ecosystem actors.

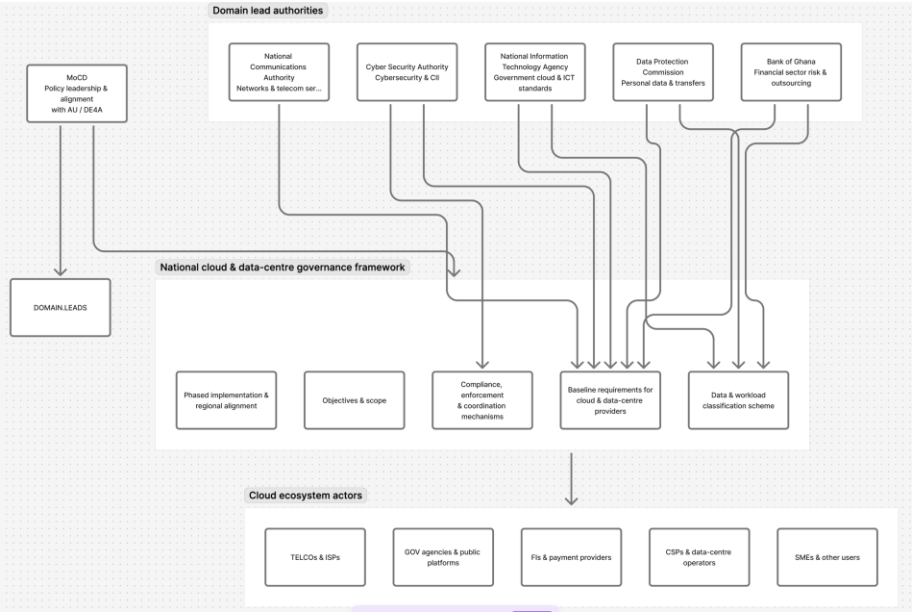

Figure 5: Proposed governance architecture for a national cloud and data-centre frameworkin Ghana.

Note. This figure outlines the proposed governance architecture with the Ministry of Communications and Digitalisation providing policy leadership; lead authorities for data protection, cybersecurity, networks, government ICT and financial-sector risk; and cloud/data-centre providers and users at the implementation layer.

For personal-data protection and cross-border transfers, the Data Protection Commission would serve as the primary authority, responsible for issuing binding guidance on data-processing obligations in cloud environments, clarifying transfer conditions and approving standard contractual clauses or other transfer tools consistent with Act 843 (Mensah, 2023). For cybersecurity and critical information infrastructure, the Cyber Security Authority would act as lead, setting minimum technical and organisational standards for cloud and data-centre environments in critical sectors, coordinating incident response and overseeing accreditation of relevant cybersecurity services. The National Communications Authority would continue to regulate networks and electronic communications services, including connectivity for data centres and cloud-service delivery, while ensuring that licence conditions and quality-of-service obligations are coherent with data-protection and cybersecurity requirements.

The National Information Technology Agency would be responsible for government cloud, national data-centre standards and ICT architecture within the public sector, including reference architectures, procurement guidelines and minimum requirements for public-sector use of commercial cloud services. In the financial sector, the Bank of Ghana would retain authority over prudential and operational risk aspects of cloud outsourcing by regulated financial institutions, but would do so in close coordination with the DPC and CSA to avoid duplicative or inconsistent demands (Adjei et al., 2021; World Bank, 2023). These relationships could be formalised in a framework agreement or memorandum of understanding, as suggested in the preceding section, to reduce fragmentation and provide a clear governance structure for cloud and data-centre oversight.

8.3 Data and workload classification

A central element of the proposed framework is a structured classification of data and workloads, which allows regulatory requirements to be calibrated to risk. Rather than imposing blanket localisation or uniform conditions on all cloud use, the framework would distinguish between at least four broad categories.

The first category would comprise routine business data and non-sensitive information, including many private-sector workloads that do not involve regulated personal data or critical functions. For these workloads, the main requirements would be compliance with general data-protection and cybersecurity obligations, irrespective of hosting location, with an emphasis on due diligence, contractual safeguards and incident management. The second category would cover regulated personal data in sectors such as telecommunications, health and basic financial services. For this category, the framework would require stronger assurances regarding data-protection compliance, cross-border transfer conditions and auditability of cloud providers, as well as explicit documentation of data flows and sub-processing arrangements in line with Act 843.

The third category would consist of critical-sector and financial-system data, including core banking systems, payment infrastructures and key telecommunications or energy control systems. For these workloads, the framework would envisage stricter conditions for hosting, such as a preference for domestic or regional data centres that meet specific resilience and oversight criteria, mandatory business-continuity arrangements and enhanced regulatory access to logs and records. The fourth category would cover national security–sensitive or specially classified government data, for which the framework could require onshore hosting in government-managed or explicitly certified facilities under NITA's oversight, with narrow and carefully controlled exceptions.

This form of classification would allow Ghana to operationalise data-sovereignty concerns in a differentiated manner, focusing stringent measures on narrowly defined high-risk categories while retaining flexibility for lower-risk workloads, in line with AU guidance to promote trusted data spaces and intra-African flows (African Union Commission, 2022; World Bank, 2023).

8.4 Requirements for cloud and data-centre providers

The framework would specify baseline requirements for cloud and data-centre providers serving Ghanaian customers or hosting Ghanaian data. These requirements would be tiered according to the classification described above but would share several common components. Providers would be expected to implement robust governance structures for information security, data protection and business continuity, aligned with recognised standards. They would need to provide clear documentation of data locations, sub-processing chains and

technical measures, enabling controllers to assess compliance with Act 843 and sectoral regulations.

For data-centre facilities operating in Ghana, the framework would build on the draft Regulatory Framework for Data Centres and relevant Smart Africa initiatives to set standards for physical security, redundancy, environmental controls, connectivity, power resilience and disaster recovery (Regulatory Framework for Data Centres, n.d.; Africa Data Centres Association & Oxford Business Group, 2024). Facilities meeting specified criteria could be certified or registered, creating a transparent tiering of data-centre quality that controllers and regulators could use when making hosting decisions. For cloud service providers, the framework would emphasise obligations to support incident reporting to Ghanaian authorities, facilitate audits where appropriate and provide contractual commitments consistent with Ghanaian data-protection and cybersecurity laws.

8.5 Compliance, enforcement and coordination

To be effective, the framework would need mechanisms for compliance monitoring, enforcement and inter-agency coordination. In line with Mensah's observation that enforcement of Act 843 has been uneven (Mensah, 2023), the proposal assumes that enforcement capacity at the Data Protection Commission, Cyber Security Authority and other bodies will need to be strengthened through dedicated budget, technical expertise and collaborative arrangements. Joint inspections, shared supervisory planning and coordinated guidance documents would be particularly important for institutions that fall under multiple regulators, such as banks, telecommunications operators and large cloud-enabled platforms.

The framework would encourage the use of soft-law tools, including guidelines, technical notes and frequently asked questions, alongside formal regulations. This is particularly relevant for fast-evolving areas of cloud technology where rigid rules risk becoming quickly outdated. Regular stakeholder consultations with providers, users, civil society and academia would support iterative refinement of requirements, consistent with the AU Data Policy Framework's emphasis on multi-stakeholder governance (African Union Commission, 2022).

8.6 Implementation and alignment with regional initiatives

Finally, implementation of the proposed framework should proceed in phases, aligned with Ghana's broader digital economy programmes and regional commitments. In the short term, emphasis could be placed on clarifying cross-border transfer guidance under Act 843,

formalising institutional coordination and adopting a basic data and workload classification scheme. In the medium term, Ghana could finalise and operationalise a regulatory framework for data centres, introduce certification mechanisms and expand government cloud standards under NITA's leadership. Over the longer term, the framework could be adjusted to reflect developments under the African Continental Free Trade Area's digital trade provisions and evolving AU data-governance instruments, with the aim of positioning Ghana as both a user and provider of trusted regional cloud and data services (African Union Commission, 2020, 2022; World Bank, 2023).

Embedding such a structured national cloud and data-centre governance framework within the broader legal and institutional reforms discussed in this paper would help move Ghana towards a more coherent, predictable and development-oriented approach to data sovereignty and cloud adoption. It would also provide a tangible, country-specific contribution to regional debates on how African states can harness cloud computing while maintaining effective control over strategic data resources.

8.7 Indicative indices for risk-based localisation, data sovereignty and self-governance

To make a risk-based approach to localisation and data sovereignty operational rather than purely conceptual, it is useful to provide organisations with simple indices that support self-assessment and internal governance. This subsection proposes three indicative tools that could be embedded in Ghana's national cloud and data-centre governance framework: a Workload Localisation Risk Index, a Data Sovereignty Assurance Index, and an Organisational Cloud Compliance Index. These indices are not intended as rigid regulatory instruments, but as structured self-governance tools that controllers can use to document decisions, demonstrate diligence and engage more effectively with regulators.

8.7.1 Workload Localisation Risk Index (WLRI)

The Workload Localisation Risk Index is designed to help organisations assess how "local" or tightly controlled a particular workload should be, based on a small set of criteria that reflect the earlier data and workload classification.

Each workload (for example, a payment switch, a student information system, a public-sector records database) is scored across four dimensions, each on a simple 0–3 scale:

a. **Data sensitivity**:
b. 0 = non-personal or low-sensitivity data;

c. 1 = ordinary personal data;
d. 2 = regulated or sector-specific sensitive data (e.g. financial, health, telecom traffic data);
e. 3 = specially protected or classified data.
f. **Criticality for continuity**:
g. 0 = non-critical, easily restorable workload;
h. 1 = important, but with acceptable downtime;
i. 2 = high criticality for organisational operations;
j. 3 = critical for national or sectoral continuity (e.g. payment system core, key public services).
k. **Regulatory exposure** (number and intensity of regulators directly involved):
l. 0 = no sectoral regulation beyond Act 843 and general law;
m. 1 = single sector regulator with limited specific requirements;
n. 2 = multiple regulators or detailed sectoral rules;
o. 3 = multiple regulators plus explicit critical-infrastructure designation.
p. **Cross-border dependency**:
q. 0 = purely domestic processing and hosting;
r. 1 = regional hosting with limited third-country processing;
s. 2 = significant reliance on global regions and third-country sub-processors;
t. 3 = complex multi-region architecture with material third-country dependence and limited substitutability.

A simple index can then be calculated as:

WLRI = (Sensitivity + Criticality + Regulatory exposure + Cross-border dependency) / 4

which yields a value between 0 and 3. The interpretation is deliberately coarse:

a. WLRI < 1.0: localisation risk is low; global or regional cloud hosting is usually acceptable, subject to baseline data-protection and security safeguards.
b. 1.0 ≤ WLRI < 2.0: moderate localisation risk; regional hosting or carefully structured global cloud arrangements may be appropriate, with stronger contractual and technical controls.
c. WLRI ≥ 2.0: high localisation risk; onshore or tightly controlled regional hosting, possibly with mirroring in a Ghana-based or AU-aligned facility and enhanced oversight, is recommended.

The index does not replace legal obligations but provides a transparent internal rationale for localisation decisions that can be documented and shared with auditors or regulators.

8.7.2 Data Sovereignty Assurance Index (DSAI)

The second instrument, the Data Sovereignty Assurance Index, shifts attention from what the workload is to how sovereignty is protected in practice. It focuses on the strength of legal, contractual and technical arrangements that ensure Ghanaian controllers retain effective control over their data, even when using foreign or regional cloud services.

Again, the index uses a small number of dimensions, each scored on a 0–3 scale for a given provider–workload combination:

1. Legal and contractual control: clarity of governing law, jurisdiction, data-processing agreements and standard clauses that reflect Act 843 requirements.
2. Transparency and auditability: ability to know where data are stored and processed, to obtain logs and evidence, and to conduct or commission audits.
3. Reversibility and exit: contractual and technical ease of data export, format portability, and guarantees on deletion and return at the end of the contract.
4. Regulatory cooperation: provider's commitment to support Ghanaian regulators (DPC, CSA, BoG, etc.) in investigations, incident management and compliance checks.

For example:

0 = no meaningful provision;

1 = basic clauses or ad hoc arrangements;

2 = reasonably robust and documented mechanisms;

3 = strong, tested mechanisms aligned with recognised best practice.

The DSAI for a workload with a particular provider can then be expressed as:

DSAI = (Legal control + Transparency + Reversibility + Regulatory cooperation) / 4

A low WLRI combined with a high DSAI suggests that cross-border cloud use is relatively safe in sovereignty terms. Conversely, a high WLRI combined with a low DSAI signals a misalignment: the workload appears high-risk, yet the current arrangements provide weak sovereignty assurances. This combination should trigger reconsideration of hosting choices or contractual terms.

8.7.3 Organisational Cloud Compliance Index (OCCI)

The third tool is an Organisational Cloud Compliance Index, a self-governance measure that reflects an organisation's internal readiness to manage cloud obligations under Act 843, the Cybersecurity Act and relevant sectoral rules. It is less about a single workload and more about organisational governance.

Indicative dimensions, again scored 0–3, could include:

1. **Governance and accountability**: presence of a designated data protection officer or equivalent, clear allocation of responsibility for cloud decisions, and documented policies for cloud use.
2. **Risk assessment and documentation**: systematic use of data-protection and security impact assessments for major cloud projects, with records retained.
3. **Vendor and contract management**: structured procedures for evaluating cloud providers, reviewing contracts against legal and regulatory requirements, and maintaining an inventory of cloud services in use.
4. **Technical and operational controls**: implementation of appropriate access control, encryption, monitoring, backup and incident-response processes tailored to cloud environments.
5. **Training and awareness**: regular training for management, IT and key business users on cloud risk, data protection and cybersecurity obligations.

An overall OCCI score can be expressed as an average or as a radar profile across these dimensions. Organisations can set internal targets (for example, a minimum average score of 2.0 before migrating critical workloads to the cloud) and track improvement over time. For regulators, such an index can support risk-based supervision: entities with low OCCI scores may warrant closer engagement or guidance.

8.7.4 Use within the Ghanaian framework

These indices are intentionally simple and can be implemented using a spreadsheet or basic internal tool. Within the proposed national cloud and data-centre governance framework, they could be used in three ways.

First, as internal compliance tools, helping controllers to document decisions about localisation and provider selection in a structured way. Second, as dialogue devices between organisations and regulators, offering a common language to discuss risk levels, sovereignty assurances and governance maturity without immediately resorting to prescriptive regulation.

Third, as potential building blocks for future regulatory instruments, should Ghana decide to formalise risk-based categories or to require large institutions to maintain documented localisation and sovereignty assessments.

When the Workload Localisation Risk Index, a Data Sovereignty Assurance Index and an Organisational Cloud Compliance Index are combined, Ghanaian organisations would be better equipped to operationalise the risk-based localisation and data sovereignty approach advocated in this study. At the same time, the indices remain sufficiently flexible to evolve as laws, regulations and regional data-governance arrangements develop.

9. Conclusion and directions for future research

This paper has examined how Ghana's existing laws, regulatory institutions and policy initiatives shape the governance of cloud computing and data, with particular attention to data sovereignty and cross-border data flows. It has shown that Ghana has put in place a substantive set of digital-era statutes such as the Electronic Transactions Act, 2008 (Act 772), the Data Protection Act, 2012 (Act 843), and the Cybersecurity Act, 2020 (Act 1038) and has established specialised institutions including the Data Protection Commission, Cyber Security Authority, National Communications Authority, National Information Technology Agency and Bank of Ghana. These, together with national digital economy strategies and emerging data-centre and cloud initiatives, these instruments provide an important foundation for secure and trusted cloud adoption.

At the same time, the analysis has identified several structural weaknesses. First, Ghana's rules for cross-border data transfers remain relatively implicit and under-specified. Act 843 sets robust general principles for personal data protection, but lacks a detailed apparatus for assessing the adequacy of foreign regimes or for structuring international transfers. In practice, this leaves controllers and cloud providers to navigate cross-border arrangements through case-by-case interactions with the Data Protection Commission and other regulators, creating uncertainty for complex, multi-jurisdictional cloud architectures. Second, responsibilities for cloud-relevant issues such as data protection, cybersecurity, critical infrastructure, outsourcing and sectoral supervision are distributed across multiple bodies, with only partial coordination and few formalised lead-agency designations. This institutional fragmentation can increase transaction costs, lengthen approval timelines and deter smaller

organisations with limited compliance capacity from undertaking substantial cloud migrations.

Third, there are persistent gaps in enforcement capacity and organisational skills. Limited resources at key regulatory bodies constrain systematic supervision and detailed technical guidance, while broader digital-skills shortages in advanced ICT, cloud architecture, cybersecurity and digital transformation limit the ability of public institutions and enterprises to design, procure and manage robust cloud solutions. These weaknesses interact with emerging data-sovereignty and localisation pressures at both national and continental levels. Without careful design, Ghana risks adopting fragmented or informally communicated localisation expectations that raise costs and reduce resilience without delivering commensurate gains in security or control; yet moving too slowly to clarify transfer rules and sovereignty principles could undermine trust and limit alignment with evolving African data-governance frameworks.

Against this backdrop, the paper has proposed a set of policy and regulatory measures. These include clarifying cross-border data-transfer rules and tools under Act 843; formalising institutional coordination and lead-agency roles for specific risk domains; developing a coherent national framework for cloud and data-centre governance that integrates data protection, cybersecurity and sectoral requirements; adopting risk-based, differentiated approaches to localisation and data sovereignty; and strengthening regulatory capacity, practical guidance and stakeholder dialogue. Collectively, these steps would move Ghana from a situation in which cloud-relevant rules and institutions exist but are partially fragmented and under-specified, to one in which cloud and data governance is coherent, predictable and aligned with both national development objectives and continental strategies.
This study has limitations that should be acknowledged. It relies entirely on secondary sources such as statutes, policy documents, regulatory instruments, continental frameworks and academic and professional commentaries and does not incorporate primary empirical work such as interviews, surveys or case studies. As a result, it cannot fully capture how regulators, cloud providers, financial institutions, public-sector agencies and other actors interpret and operationalise the legal framework in practice. In addition, the legal and policy landscape in Ghana is evolving: proposed reforms to communications and ICT legislation, emerging data-centre regulations and new regional initiatives may reshape the terrain in ways that this analysis can only partially anticipate.

These limitations point to several directions for future research. One avenue is qualitative empirical work that explores how regulators, cloud providers and institutional users understand and manage cloud-related obligations, including decisions about data location, cross-border transfers and incident reporting. Another is comparative research that situates Ghana's framework alongside those of other African countries, examining different models of institutional coordination, data-sovereignty strategies and cloud regulation. A third priority is longitudinal analysis of legal and policy reforms, tracking how new statutes, guidelines and regional instruments affect cloud adoption, market development and the balance between sovereignty and openness over time.

By mapping Ghana's current legal and institutional landscape for cloud computing and data governance and by clealry linking it to a wider data-sovereignty debates in Africa, this paper provides a foundation for these future inquiries. It also offers policymakers, regulators and industry stakeholders a structured view of the strengths, gaps and opportunities in Ghana's cloud governance framework at a moment when decisions about data, infrastructure and sovereignty will be critical to the country's digital transformation trajectory.

Limitations of the study

This study has several limitations that should be acknowledged when interpreting its findings and proposals. First, the analysis is based entirely on secondary sources: statutes, policy documents, regulatory instruments, continental frameworks, official reports and existing academic and professional commentary. It does not incorporate primary empirical evidence such as interviews with regulators, industry stakeholders and service providers, or detailed case studies of specific cloud deployments in Ghana. As a result, the paper cannot fully capture how the legal and institutional framework is interpreted and applied in day-to-day regulatory practice, contract negotiation or technical design.

Second, the legal and policy environment examined here is dynamic rather than static. Ghana is in the process of updating elements of its communications and ICT legislation, developing a regulatory framework for data centres and participating in evolving African Union and Smart Africa initiatives on data and cloud governance. Any desk-based snapshot is therefore inherently time-bound. Some of the recommendations and the proposed national cloud and data-centre governance framework may need to be adapted as new laws, regulations or regional instruments are adopted, consolidated or judicially interpreted.

Third, while the paper draws on comparative and continental sources, its scope is deliberately national and doctrinal. It focuses on Ghana's statutes and institutions and situates them within African data-sovereignty debates, but it does not undertake a systematic comparative analysis of alternative models in other African or non-African jurisdictions. Nor does it quantify the impact of particular legal or institutional features on cloud adoption outcomes. The discussion of risks, challenges and potential benefits is therefore primarily qualitative and conceptual, rather than econometric or statistically validated. Fourth, the indices for risk-based localisation, data sovereignty and self-governance proposed in the later sections are explicitly normative and illustrative. They have not been empirically tested with Ghanaian institutions, calibrated through structured expert elicitation, or validated against real-world adoption and compliance outcomes. They should therefore be treated as heuristics and starting points for further refinement, rather than as ready-made regulatory instruments or industry standards.

Finally, although the paper engages with African Union strategies, AU data-policy instruments and regional data-centre analyses, it does not fully address broader political economy factors such as bargaining power between states and large cloud providers, regional infrastructure asymmetries, or the influence of trade and investment agreements on data-governance choices. These dimensions are likely to shape the feasibility and trajectory of any national framework in practice. These limitations do not undermine the core contribution of the study which is a structured mapping of Ghana's cloud-relevant legal and institutional landscape and a concrete proposal for a national cloud and data-centre governance framework but they do suggest that the findings should be read as a conceptual and policy design input, to be complemented by empirical research, stakeholder engagement and iterative regulatory practice.

REFERENCES

1. Adjei, J. K., Adams, S., & Mamattah, L. (2021). Cloud computing adoption in Ghana: Accounting for institutional factors. *Technology in Society, 65*, 101583. https://doi.org/10.1016/j.techsoc.2021.101583
2. Africa Data Centres Association. (2023). *Africa interconnection report 2023*. Africa Data Centres Association.
3. Africa Data Centres Association, & Oxford Business Group. (2024). *Africa Data Centres Association – Market report 2024*. Africa Data Centres Association.

4. African Union Commission. (2014). *African Union Convention on Cyber Security and Personal Data Protection*. African Union.
5. African Union Commission. (2020). *Digital Transformation Strategy for Africa (2020–2030)*. African Union.
6. African Union Commission. (2022). *AU Data Policy Framework*. African Union.
7. Bank of Ghana . (2024, Outsourcing Directive.
8. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.bog.gov.gh/wp-content/uploads/2024/11/BOG-Outsourcing-Directive.pdf&ved=2ahUKEwiGnO7l6a2RAxVRUEEAHSwGAUEQFnoECB4QAQ&usg=AOvVaw1gRNCuJJrzfZphxOE6rsb
9. Coffie, C. P. K., Hongjiang, Z., Mensah, I. A., Kiconco, R., & Simon, A. E. O. (2021). Determinants of FinTech payment services diffusion by SMEs in Sub-Saharan Africa: Evidence from Ghana. *Information Technology for Development, 27*(3), 539–560. https://doi.org/10.1080/02681102.2020.1840324
10. DLA Piper. (2024). *Data protection laws of the world: Ghana*. In *Data Protection Laws of the World Handbook 2025*. DLA Piper.
11. European Union. (2016). 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).
12. Ghana Statistical Service, & National Communications Authority. (2020). *Household survey on ICT in Ghana (2019): Abridged report*. Ghana Statistical Service & National Communications Authority.
13. International Telecommunication Union. (2023). *Measuring digital development: Facts and figures 2023*. ITU.
14. Joseph, Z. B., Mensah, K. B., & Abraham, Z. N. (2023). Data privacy regulations in Ghana: A guide to GDPR compliance for businesses. *Journal of Legal Subjects, 3*(4), 32–41. https://doi.org/10.55529/jls.34.32.41
15. Mensah, N. A. B. (2023). *An overview of the Data Protection Act of Ghana: Examining the legal framework for data outsourcing* [Unpublished manuscript]. University of Ghana.
16. Ministry of Communications and Digitalisation. (2023). *Ghana Digital Economy Policy and Strategy*. Government of Ghana.

17. National Information Technology Agency. (2023, November 15). *Inaugural stakeholder engagement meeting (virtual): National data centre and cloud regulatory framework development – Smart Africa support to Ghana*. National Information Technology Agency.
18. Pazarbasioglu, C., García Mora, A., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). *Digital financial services*. World Bank Group.
19. Republic of Ghana. (1992). *Constitution of the Republic of Ghana*. Ghana Publishing Company.
20. Republic of Ghana. (2008). *Electronic Transactions Act, 2008 (Act 772)*. Ghana Publishing Company.
21. Republic of Ghana. (2012). *Data Protection Act, 2012 (Act 843)*. Ghana Publishing Company.
22. Republic of Ghana. (2020). *Cybersecurity Act, 2020 (Act 1038)*. Ghana Publishing Company.
23. Republic of Ghana. (2023). *National Artificial Intelligence Strategy of Ghana*. Government of Ghana.
24. Senyo, P. K., Karanasios, S., Gozman, D., & Baba, M. (2022). FinTech ecosystem practices shaping financial inclusion: The case of mobile money in Ghana. *European Journal of Information Systems, 31*(1), 112–127. https://doi.org/10.1080/0960085X.2021.1978342
25. Smart Africa. (2022a, April 5). *SADA conducts workshops in Ghana to strengthen data centres and cloud services ecosystem*. Smart Africa Digital Academy.
26. Smart Africa. (2022b). *The role of African governments and multilateral organizations in increasing the footprint of multi-tenant data centres and cloud infrastructure in Africa*. Smart Africa.
27. Templars. (2023). *Data protection compliance in Ghana: Navigating the regulatory framework and emerging compliance requirements*. Templars.
28. World Bank. (2020). *Digital Africa: Technological transformation for jobs*. World Bank.
29. World Bank Group. (2019). *Ghana Digital Economy Diagnostic: Stock-taking report*. World Bank Group.
30. World Bank Group. (2023). *Digital Economy for Africa (DE4A) initiative: Ghana country updates*. World Bank Group.
31. World Trade Organization. (2024). *Digital trade review and next steps for Ghana under the Digital Trade for Africa initiative*. WTO.