dga ALBRIGHT STONEBRIDGE GROUP

Stay ahead with us.

Insights

Saudi Arabia's New Digital Economy: The Kingdom Makes Strides in Data Monetization, Cybersecurity, and AI Policy

dgagroup.com

July 2026

Key Takeaways

The Saudi Council of Ministers designated 2026 as the Kingdom's "Year of Artificial Intelligence" in March, reflecting a government-wide refocusing of priorities and spending toward making Saudi Arabia a global AI hub. In the months since, the Saudi Data and Artificial Intelligence Authority and other technology regulators have issued a flurry of new policies and consultations, including the **Responsible AI Policy**, the draft **AI-First Policy**, the **National AI Risk Management Framework**, the draft **AI Cybersecurity Guidelines**, the draft **Enterprise Architecture Implementation Controls**, the **Data Monetization Policy**, and **three Personal Data Protection Law-related draft consultations**.

Collectively, these policies signal important long-term trends in the policy landscape, including:

- **The digital economy remains central to Saudi Arabia's non-oil growth strategy.** AI adoption, data monetization, and digital government services are core parts of the Kingdom's broader effort to diversify away from oil, create new sources of public revenue, and generate more durable economic returns.
- **Saudi Arabia is pursuing AI through both acceleration and control.** The draft AI-First Policy issued by SDAIA for public consultation pushes AI adoption as a top priority for government entities, while the Responsible AI Policy and National AI Risk Management Framework aim to establish guardrails for safe, accountable, and risk-based use.
- **The Kingdom is opening a controlled marketplace for government data products.** Published in June, SDAIA's Data Monetization Policy creates a path for government data to generate revenue through licensed data products and services, but it prohibits the direct sale of raw government data. This reflects a controlled approach to data commercialization.
- **The Kingdom is using non-binding regulatory instruments to signal the future regulatory direction.** While some of the newly issued policy frameworks, such as the AI Risk Management Framework, are non-binding, they provide a clear indication of the government's policy priorities and direction and are likely to be followed in time by binding regulatory instruments.
- **Companies have commercial opportunities but must position themselves as compliant implementation partners.** Foreign and domestic companies can support Saudi Arabia's AI and data agenda by offering AI governance, cybersecurity, data productization, and modernization services. However, they will need to align with Saudi data protection and oversight expectations.

Table — New AI and Data Regulatory Instruments

Regulatory Instrument	Content	Context
AI-First Policy (SDAIA)	• Aims for AI to be the default consideration for public sector services and operations. • Applies to government entities primarily and encourages responsible adoption that incorporates human oversight and data protection.	Issued for public consultation, which closes on **July 28, 2026.**
AI Cybersecurity Guidelines (NCA)	• Lists recommended cybersecurity guardrails across AI design, development, and deployment. • Covers generative and agentic AI model training and inference data, applications, APIs, and other related tools.	Issued for public consultation, which closes on **August 5, 2026**.
Accreditation Certificate Standards Guide for Data Controllers and Processors (SDAIA)	• Sets the criteria for assessing and accrediting controllers and processors' PDPL compliance.	Issued for public consultation, which closes on **August 6, 2026**.
Accreditation Certification Activities Licensing Standards Guide (SDAIA)	• Sets standards for entities seeking licenses to issue accrediting certificates.	Issued for public consultation, which closes on **August 6, 2026**.
Audit and Inspection Activities Licensing Standards Guide (SDAIA)	• Establishes licensing standards for entities that audit or inspect personal data processing activities.	Issued for public consultation, which closes on **August 6, 2026**.
Enterprise Architecture Implementation Controls (DGA)	• Requires enterprise architecture, including a Chief Enterprise Architect and an associated team, to work across business applications. • Introduces common standards across governance, training, and reporting.	Issued for public consultation, which closes on **August 14, 2026.**
Responsible AI Policy (SDAIA)	• Establishes broad responsible AI obligations for developers, users, and publishers of AI systems. • Creates a risk tiering system, system registration requirements, AI ethics labelling, audit and assurance obligations, and a regulatory sandbox. • Applies across government, private, and non-profit actors.	Publicly consulted on from April to June 2026.
Data Monetization Policy (SDAIA)	• Creates a framework for government entities to monetize government data through value-added products and services. • Establishes government data as a national asset, prohibits the sale of raw data, and limits private sector access to licensed approved purposes.	Issued on June 19, 2026.
National AI Risk Management Framework	• Provides an AI risk management model across the lifecycle through a probability impact score matrix. • Encourages organizations to identify, assess, treat, and continuously monitor risks. • While not binding, this framework will likely impact future regulations in the AI risk management space.	Released on July 14, 2026.

Introduction

On March 10, 2026, following formal approval from the Council of Ministers, Saudi Arabia officially declared 2026 as the "Year of Artificial Intelligence". Since then, the Saudi Data and Artificial Intelligence Authority and adjacent regulators have issued a range of data and AI regulatory instruments, ranging from guidelines to policies, that is pushing the Kingdom towards a new era of data protection and AI adoption.

Saudi Arabia's digital ambitions are not new; the Kingdom has pursued digital transformation initiatives since the 1970s. What has changed is the urgency: As the Kingdom reckons with the limits of capital-intensive mega-projects and a recent regional conflict that has made these fiscal pressures more acute, the digital economy offers a clearer path to higher long-term returns. Given Saudi Arabia's Vision 2030 objective of expanding economic diversification and non-oil government revenue through investments, fees, and penalties, technology has become central to both its growth strategy and its fiscal resilience.

Below, we explore the origins of Saudi Arabia's digital transformation and the newfound regulatory instruments the Kingdom is implementing as a part of the year of AI.

The Institutional Buildout

Saudi Arabia's digital transformation began in 1979 with the Ministry of Interior's Computer Center and later expanded through Yesser, Absher, and the GOV.SA portal, digitizing many core government services by the 2012–2016 e-government strategy cycle. The launch of Vision 2030 turned these efforts into a broader national reform agenda focused on expanding digital services across all sectors and broadband expansion. That foundation has delivered tangible results: Saudi Arabia ranked 6th globally in the UN's 2024 E-Government Development Index, and internet use among people aged 15–74 reached roughly 99% in 2025, with about 98% using online government services. These achievements now underpin the Kingdom's wider data and AI ambitions.

As Saudi Arabia's digital economy has matured, the Kingdom has built the institutional framework to govern it.

The **Saudi Data and Artificial Intelligence Authority** (SDAIA) is the Kingdom's most important regulator for data and AI. Established by Royal Order in 2019, SDAIA leads the national data and AI agenda under Vision 2030, with a mandate covering data governance, AI development, and the regulation and application of data and AI across the Kingdom. It oversees three agencies: the **National Data Management Office** serves as the legislative and governance arm, the **National Information Center** operates national data infrastructure, and the **National Center for AI** drives AI research, innovation, and deployment. SDAIA's work is guided by the National Strategy for Data & AI, which sets 2030 targets including placing Saudi Arabia among the world's top 15 AI nations, attracting around $20 billion in data and AI investment, developing 20,000 specialists and experts, and supporting 300 startups.

The **Digital Government Authority** (DGA) is the Kingdom's most important regulator for digital government services. Established in 2021 after earlier e-government initiatives, such as Yesser, were absorbed into its mandate, DGA leads public-sector digital transformation. It is responsible for digital government regulation, standards, performance measurement, cross-government integration, cloud operations, digital procurement, licensing frameworks, and emerging technology strategies. Through tools such as the Basic Standards of Digital Transformation, the Qiyas annual review, and the Digital Experience Maturity Index, DGA sets benchmarks for how government entities digitize and deliver services.

The **National Cybersecurity Authority** (NCA) also plays an important supporting role by setting cybersecurity controls and incident-response frameworks, monitoring compliance, regulating sensitive cyber activities, and implementing Saudi Arabia's National Cybersecurity Strategy. While NCA is primarily a national security body, its work increasingly shapes the guardrails for AI and digital transformation across the Kingdom.

Saudi Arabia's AI and Data Policies in the Year of AI

Saudi Arabia's New AI and E-Government Instruments

Saudi Arabia's 2026 AI agenda reflects a dual strategy: accelerating AI adoption while building the governance, cybersecurity, privacy, and risk controls needed to manage it responsibly. Saudi Arabia has driven this agenda through the following instruments.

- SDAIA's draft **AI-First Policy** encourages AI integration across government agencies and their respective internal and external operations. It emphasizes responsible AI governance, human oversight, data protection, cybersecurity, and the organizational capabilities needed to support effective AI implementation, including governance structures, skilled talent, quality data, and national AI infrastructure.
- The NCA is adding another layer of oversight through its draft **AI Cybersecurity Guidelines**. Although non-binding, they are likely to influence future regulatory expectations. The guidelines cover the full AI lifecycle, including generative and agentic AI systems, and focus on key controls over four areas: cybersecurity governance, defense, resilience, and third-party risk.
- SDAIA's **Responsible AI Policy** sets broad obligations for AI development and use across government, private sector, non-profit, and individual actors, combining responsible design duties with risk-based classification.
- The **National AI Risk Management Framework** gives organizations a lifecycle-based model to identify, assess, treat, and monitor AI risks. Companies with AI products in the Kingdom are encouraged to provide use-case-specific AI risk assessments, documentation of intended and prohibited uses, data-protection materials, escalation mechanisms, bias controls, incident-response procedures, and clear evidence of compliance with Saudi data and sector regulations.

The DGA is also strengthening e-government services delivery through its draft **Enterprise Architecture Implementation Controls**. The controls seek to standardize how government entities apply the National Enterprise Architecture Methodology and require entities to establish enterprise architecture functions, appoint a Chief Enterprise Architect, and adopt governance and control processes. The policy aims to coordinate government digital projects and align technology investments with national architecture requirements.

Saudi Arabia's New Data Regulatory Instruments

Saudi Arabia is also moving to unlock the economic value of government data while keeping it within a controlled regulatory framework.

The **Data Monetization Policy** allows government entities to commercialize data products to generate revenue but prohibits the direct sale of raw government data. The private sector's access to these data products is limited to licensed and approved purposes only. Government data must be managed in the public interest, and existing policies surrounding freedom of information, intergovernmental data sharing, and personal data protection continue to apply. Even with a newfound government data marketplace, the Personal Data Protection Law (PDPL) takes precedence. SDAIA has continued to build out compliance infrastructure around the PDPL through three consultations that close on August 6, 2026:

1. **Accreditation certificates for controllers and processors,** allowing organizations to evidence PDPL compliance through standardized certification, including National Register listing, documented controls, DPO designation, and evaluation by licensed certifiers.
2. **Licensing standards for certification bodies,** setting requirements for entities that issue compliance certificates, including local establishment, accreditation, capital, staffing, and license conditions.
3. **Licensing standards for auditors and inspectors,** creating a supervised market for PDPL auditing and inspection activities, including local data retention obligations and ongoing self-assessment requirements.

Together, these measures support Saudi Arabia's data sovereignty ambitions by enabling domestic data-driven value creation while clarifying how data must be handled, verified, retained, and protected.

Implications for Policymakers and Government Entities

Government entities should embrace implementing AI solutions and data modernization in line with the Kingdom's evolving policy direction, while ensuring that adoption remains compliant, secure, and properly governed.

- **Create a strategy.** New technology guidelines should serve existing government objectives, not drive them. Governments need to have an internal strategy for implementing new AI solutions and monetizing data products to ensure that their efforts are in line with their audit.
- **Identify your customers.** Governments need to identify who their customers are for their data products and cater to these buyers. Otherwise, government entities risk wasting internal resources on low-return products.
- **Avoid additional red tape.** Government entities need to be wary of creating more bureaucratic burdens, either for companies interested in their data products or for users of their public services. Government entities should assess existing requirements for AI implementation and data monetization to see what is necessary to implement, and what would prevent users or customers from engaging.
- **Know your red lines.** For government entities with sensitive raw data, entities should be clear on what data can be used as a part of a data product and what data needs to stay private regardless of the monetization opportunity.

Implications for Companies

Companies have an opportunity to position themselves as implementation partners in Saudi Arabia's AI and data transformation agenda, particularly across cybersecurity, data monetization, compliance, digital infrastructure, and public sector modernization initiatives.

Companies should also treat current consultations and guidelines as important indicators of the likely direction of future policy, regulatory expectations, and procurement requirements in the sector.

- **Be a trusted ally.** With the right engagement strategy, companies can assist with government service and systems automation, the creation of data products, and sector-specific AI tools.
- **Understand new needs.** With the continued emphasis on responsible AI deployment and risk management, companies with specialized capabilities are well positioned to pitch their services to government entities that will increasingly need risk management and explainability integrated into their technology solutions.
- **Implement data protections.** PDPL has been a major cornerstone of Saudi data regulation since 2023, and the new public consultations on the accreditation certification alongside licensing requirements for auditors and certifiers signals a continued push for PDPL enforcement in the Kingdom. Companies should conduct thorough reviews to ensure their compliance with the PDPL and its accompanying web of regulations.
- **Be prepared.** While several of the new AI regulatory instruments are nonbinding, these frameworks signal the Kingdom's future AI policy direction, and voluntary compliance can signal support for the Kingdom's digital modernization goals. Companies providing AI products or solutions should undergo reviews of their internal AI risk and oversight protocols to ensure that the direction of their internal policy aligns with the published frameworks.

Looking Ahead

In line with the direction Saudi Arabia has already taken during its "Year of Artificial Intelligence," Riyadh will likely continue to expand regulatory oversight of AI products while also encouraging wider AI adoption across the Kingdom. This creates both opportunities and pressure points for government entities and companies. Government entities will be expected to deliver tailored AI-enabled products and services that improve public-sector performance and contribute to non-oil revenue growth. Several ministries have already kicked off AI initiatives, such as the Ministry of Tourism's AI Tourism Vision and the Ministry of Commerce's adoption of HUMAIN's NVIDIA B300 AI cluster, which will likely create pressure for other ministries to follow suit. Meanwhile, companies will face a growing set of data protection obligations, licensing procedures, and responsible AI expectations, both as a baseline for operating in the Kingdom and to showcase alignment with Saudi Arabia's long-term digital economy objectives.

As the Kingdom moves into the second half of the "Year of AI," government entities and companies alike should prepare for a regulatory environment that is increasingly focused on both accelerating and governing the growth of Saudi Arabia's digital economy.

About Us

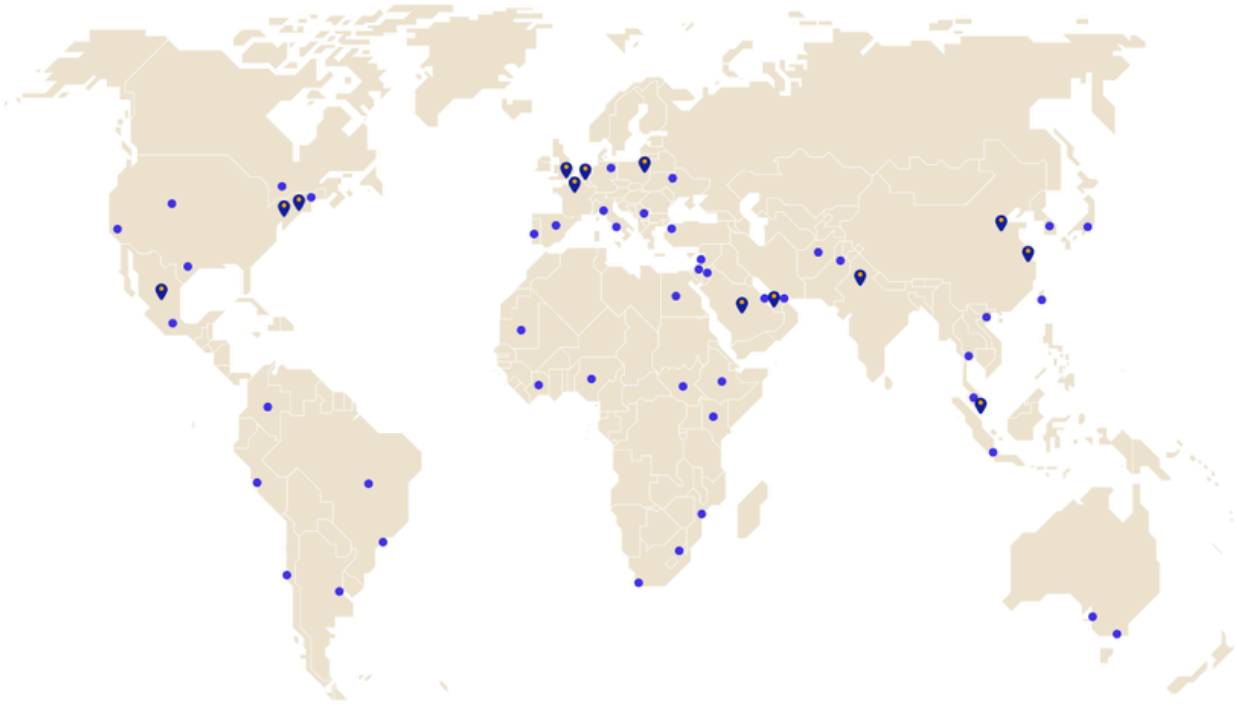
DGA Group is a global advisory firm with deep expertise and longstanding experience around the world, supporting companies and governments with a focus on regulatory capacity building, public policy, government relations and strategic communications. Our technology policy and strategy team assist multinational companies and governments alike on regulatory and geopolitical advisory, national strategy, and AI policy and governance. In Saudi Arabia, we help companies navigate a wide range of high-impact regulatory policy issues where market access and business growth are at stake, including EPP, Regional Headquarters (RHQ), and other local content mechanisms.

To learn more, visit dgagroup.com. Please contact us with any questions or to arrange a follow-up conversation.

Imad Al-Abdulqader
Partner
Imad.AlAbdulqader@dgagroup.com

Alexis Serfaty
Managing Director
Alexis.Serfaty@dgagroup.com

Kristin Zhu
Associate
Kristin.Zhu@dgagroup.com



Global coverage for global needs.
13 offices | 46 extended locations