DENTONS GLOBAL ADVISORS

ASG ALBRIGHT STONEBRIDGE GROUP

Public Consultation in Saudi Arabia for Data Sovereignty

ASG Analysis

March 28, 2024

Key Takeaways

- Saudi Arabia's Vision 2030 integrates data governance, digital infrastructure, cloud adoption, and data sovereignty towards its national transformation objectives.

- The Saudi Data and Artificial Intelligence Authority is seeking public input through three ongoing consultations. One focuses on data sovereignty and its four key principles for policy development while the other two involve data sharing. Companies are encouraged to participate in these consultations that shape future regulations. By closely monitoring evolving regulations, businesses can identify both market opportunities and potential operational impacts.

- The Data and Artificial Intelligence Authority's data sovereignty consultation reflects a growing trend in the Gulf Cooperation Council (GCC) to address escalating cyberattacks through data governance and regional cooperation.

- Saudi Arabia's data governance strategy highlights data localization, similar to India and the European Union, whose approaches aim to protect citizen data, control digital assets, and boost the economy. Balancing national security and economic interests with the benefits of a free-flowing digital economy remains a challenge.

- There is a global shift towards 'trusted data flows' over strict data localization. Initiatives like the G7's "Data Free Flow with Trust" framework promote interoperable data governance systems that respect privacy, security, and intellectual property. Saudi Arabia may consider these international developments while drafting its own data sovereignty policies.

How Saudi Arabia manages its data assets

The evolution towards digitalization and the associated considerations of data governance are integral to the ambitions outlined in Saudi Arabia's Vision 2030. The national agenda, aimed at economic diversification, emphasizes the transition to a more data-centric economy. Central to this shift is the importance of data sovereignty, bolstered by robust digital infrastructure and widespread adoption of cloud technologies. The strategic integration of data sovereignty is pivotal as Saudi Arabia endeavors to enhance connectivity across governmental, industrial, and academic spheres, aligning with the overarching objective of steering away from reliance on hydrocarbons towards a data-driven sustainable economic model.

While sector-specific regulators bear distinct responsibilities in terms of data governance, the Saudi Data and Artificial Intelligence Authority (SDAIA) assumes a fundamental role in driving the national agenda concerning artificial intelligence and big data. With the release of its National Strategy for Data and Artificial Intelligence in 2020, SDAIA aimed to significantly elevate the sector's GDP contributions to $133.3 billion by 2030. Key entities under SDAIA's purview include the National Center for Artificial Intelligence, the National Data Management Office, and the National Information Center.

Concurrently, the National Cybersecurity Authority (NCA) safeguards Saudi Arabia's interests in cyberspace, including the protection of citizen data and corporate intellectual property. The launch of the National Portal for Cybersecurity Services (HASEEN) in 2022 underscored NCA's commitment to enhancing cybersecurity infrastructure, facilitating real-time information sharing, and fostering compliance with best practices among entities.

Furthermore, the government's ongoing information and communication technology (ICT) sector development strategy, initiated in 2023, has aimed to significantly elevate the sector's contribution to GDP by $13 billion, expand the information and emerging technologies market by 50%, and generate over 25,000 ICT-related jobs. The strategy, serving as a roadmap for digital transformation across the Kingdom, encompasses the implementation of national data policies. Multiple government bodies collaborate to realize the objectives outlined in the ICT sector development strategy, with the Communications, Space, and Technology Commission (CST) assuming a central role in bridging governmental and private sector interests, including both traditional telecoms and emerging technology segments.

As governments worldwide navigate rapid advancements in digital technologies, particularly with the swift evolution of AI, Saudi Arabia is intent on remaining at the forefront of digital transformation. In 2022, the Kingdom unveiled a comprehensive ICT law (Royal Decree No. M/106) encompassing telecommunications and information technology sectors whose legislation addressed digital infrastructure, e-governance, emerging technologies, and the facilitation of applications and services. One notable provision mandated adherence to Saudi Arabia's newly established personal data protection law (PDPL), initially proposed in 2021 and enacted in 2023 following a public consultation led by SDAIA. The consultation process led to amendments, particularly concerning regulations surrounding international data transfers, and the revised provision offered more flexibility for data controllers to transfer personal data abroad or disclose data to entities outside Saudi Arabia, provided such actions do not compromise national security or vital interests. Additionally, the updated law enhanced individuals' rights by simplifying the process for requesting the deletion of personal data (see our previous Analysis).

Public consultation for policy drafting with four fundamental principles

In a move to solidify Saudi Arabia's leadership in data governance, SDAIA released a Data Sovereignty Draft Public Policy for public consultation on March 10, 2024. This open forum, available until April 9, seeks feedback from a wide range of stakeholders to inform the development of related legislation.

The draft policy outlines the Kingdom's four fundamental principles for data sovereignty and welcomes public comments. The consultation process, similar to the one used for the revised PDPL, can impact policy formation. Feedback channels are spread widely, including through business forums like the U.S. Chamber of Commerce, which will collect and submit comments on behalf of its member companies.

The four principles are meant to clearly express the general direction of policy development that all government entities and the private sector should consider. Once the data sovereignty policy is approved and finalized, it is expected that more specific initiatives will follow, which could include sector-specific regulations.

First principle: data as a national asset

Saudi Arabia recognizes data as a national asset crucial for economic growth and leadership in a data-driven world. To achieve this, the Kingdom prioritizes data sovereignty through enforcing its own data regulations and governance models. Additionally, it emphasizes transparency by establishing clear rules for public access to non-classified government data and promotes open data practices to foster innovation and economic development, all within the framework of established legal guidelines.

Second principle: data protection

Saudi Arabia prioritizes data security through regulations that protect against breaches and unauthorized access. This includes safeguarding non-personal data deemed critical national infrastructure, as well as personal data handled by various entities. The Kingdom aims to implement best practices for granting access to government employees based on their specific needs, while also upholding individual privacy rights through established legal frameworks.

Third principle: data availability

Saudi Arabia seeks to establish best practices for data access by both domestic and foreign competent authorities. This includes ensuring timely access for its own authorities and fulfilling international legal obligations, all within the country's existing legal framework. Additionally, the Kingdom prioritizes developing plans for data recovery and business continuity for public entities in case of emergencies.

Fourth principle: encouragement of local and foreign investment

Recognizing data as a key driver for economic growth, Saudi Arabia aims to create an attractive investment environment. Through new regulations, the Kingdom seeks to attract foreign digital investment, prevent monopolies, and strengthen local businesses. This strategy also focuses on supporting innovative domestic digital companies that can compete regionally and globally. The Kingdom seeks this growth within a framework that safeguards national data sovereignty.

Other ongoing public consultations regarding data sharing

SDAIA’s public consultation on data sovereignty comes amid two other ongoing public consultations around data governance also released by this same government agency.

The first, titled Regulation on Personal Data Transfer Outside the Kingdom, announced on March 19 and available for feedback until April 18, involves draft amendments to data privacy regulations that provide more details and rules, particularly around exemptions, transfers after exemptions, and risk assessments. The amendments clarify what constitutes "appropriate safeguards" for data transferred outside Saudi Arabia, simplify transfer purposes, and set stricter standards for assessing data protection in other countries. They also give the authorities more power to oversee transfers and revoke exemptions if needed. Establishing a process for re-evaluating risk in cases where safeguards disappear or high risks arise, they outline how the authorities will assess a country’s data protection level and update the list of approved countries for data transfers.

The second public consultation, titled Data Sharing Policy Amendments, outlines updates to how government entities in Saudi Arabia share data with each other. Also available for consultation until April 18, the policy defines key terms, clarifies to whom it applies, and establishes eight core principles for responsible data sharing. These principles focus on participation, avoiding data redundancy, legal use, authorized access, transparency, shared accountability, data security, and ethical use. The policy details the steps involved in the data sharing process, including request submission, approval procedures, defining data controls and timeframes, and assigns roles and responsibilities to involved parties and the National Data Management Office (NDMO) for oversight and dispute resolution.

That SDAIA released three overlapping and simultaneous public consultations further underscores its intent to refine national-level policies for overall data governance and generates expectations for the implementation of additional sector-specific guidelines in the future.

Regional momentum towards security of digital assets

SDAIA's public consultation on data sovereignty builds on a growing trend across the GCC to implement data governance that addresses and mitigates escalating cybersecurity challenges. The rise in global cyberattacks since the early 2010s targeting businesses and governments alike has spurred the GCC to develop more comprehensive cybersecurity strategies.

This focus is well-placed. According to Edge Middle East, a regional technology publication, the total cost of data breaches for organizations in the Middle East reached an all-time high of $8 million in 2023, an increase of 156% over the past decade. Recognizing the regional nature of the threat, GCC countries are fostering cooperation. In October 2022, cybersecurity heads from all six GCC nations convened in Riyadh for the first meeting of the GCC Ministerial Committee for Cybersecurity. The inaugural meeting resulted in plans for joint cybersecurity exercises, promoting the exchange of information and expertise to bolster regional defenses.

International momentum on data sovereignty and localization: implications for Saudi Arabia

As Saudi Arabia ramps up data governance efforts, particularly through soliciting public feedback on its recently released data sovereignty strategy, it will be important to understand how international discussions on this issue are evolving. While there is no silver bullet data governance regime, and countries outside the region have chosen to adopt varied approaches to data sovereignty, there are some important international developments that could inform the Kingdom's forthcoming policies on data sovereignty.

Overall, Saudi Arabia's data governance strategy appears to mirror those of other countries that have adopted data localization laws. The recent public consultation highlights that its regulatory approach is motivated by similar concerns to countries and regions like India and the EU, including a desire to protect citizen data, assert control over digital assets, and harness economic benefits. But how these four overarching principles will be translated into policy will ultimately determine Saudi Arabia's ability to set a fine line between protecting national security and economic interests and securing the benefits of the digital economy.

Globally, debates over data sovereignty and cross-border data flows have intensified over the last few years, with countries refining their approaches to data localization and cross-border data flows in the face of significant criticisms of these policies. A case in point is India, which significantly watered down the data localization requirements in the final version of the Digital Data Protection Act (DDPA) in 2023 following widespread industry criticism about the impact that requirements would have on the cost of doing business and foreign direct investment (FDI) inflows into the country. Indian startups also played a major role in the decision to walk back the country's data localization requirements, as they argued that the law would place disproportionately onerous obligations on small- and medium-size enterprises using third-party cloud service providers. Similarly, Vietnam significantly narrowed the data localization requirements in its cybersecurity law in 2019 due to criticism that the law would make the country more vulnerable to cyber threats and hinder the expansion of the digital economy.

China has one of the world's most developed cyber and data governance frameworks, and most of it is predicated on data sovereignty, and this has informed Beijing's policy-making decisions when it comes to data protection and localization. China's Cybersecurity Law and Data Security Law demand that any data that is deemed important to the country must be stored within China's borders. Any data in this category that needs to leave the borders of the PRC theoretically must go through security assessments by local authorities. Some information that might not necessarily be seen as critical by the rest of the world, such as shopping preferences of a driver in an intelligent connected vehicle, is treated as important data by China and is required to be localized. The exact list of what is categorized as important data has been nebulous; and kept purposefully so—nominally because authorities say that the nature of data changes over time, but also because Beijing can retain the right to block cross-border data access should they see the national security need to do so. Due to significant pushback from foreign companies, authorities have recently significantly relaxed China's cross-border data transfer requirements and have also signaled that the country would be willing to set up pilot zones for more open data transfer.

At the multilateral level, efforts to facilitate free and open digital trade are expanding. Debates over cross-border data flows have been particularly significant in forums like the G7, with member states advocating that countries adopt "trusted data flows" over data localization laws. In 2019, for instance, former Japanese President Shinzo Abe proposed the "Data Free Flow with Trust" (DFFT) framework, which aims to establish a trusted and interoperable global governance system for data underpinned by trust in privacy, security, and intellectual property. Since then, the Group of Seven (G7) countries have been actively working to operationalize this framework. In 2021, the group laid out a "Roadmap for Cooperation" across four key areas, including data localization, regulatory cooperation, government access to data, and data sharing in priority sectors and, more recently, at the Hiroshima Summit in 2023, G7 members established the Institutional Arrangement for Partnership (IAP) to operationalize the DFFT. While it is true that the DFFT still faces a long road to implementation, G7 commitments to operationalizing the framework underscore the importance that countries are placing on free cross border data flows.

It is worth noting, however, that global data governance rules remain a patchwork of trade agreements and principles that are not universally accepted or applied. Therefore, until national data governance systems are interoperable, and countries agree on international standards on privacy, individual nations will craft their own data governance regimes. Saudi Arabia is no exception. However, as the Kingdom looks to map out its data sovereignty policies, it should monitor international developments closely. It should also consider the following questions:

- How could future data sovereignty policies impede existing bilateral data sharing agreements and other trade relationships?
- How would future data sovereignty policies affect data-driven commercial activities such as e-commerce for the Kingdom?

- What impacts would data sovereignty policies have on foreign direct investment, business operations, and overall business competitiveness in the Kingdom?
- How would future data sovereignty policies affect technological growth in emerging technologies, such as cloud infrastructure and artificial intelligence model training?
- What other third-order impacts could data sovereignty policies have on the business environment in the Kingdom? For example, what are the compliance costs the Kingdom expects foreign businesses to adopt with future policies?
- To what extent would forthcoming policies create friction between the Kingdom and its trading partners?
- How would the Kingdom set up best practices for data protection and cross-border data transfer with future data sovereignty policies?
- How could forthcoming policies fit with existing multilateral frameworks on cross-border data flows?

ABOUT US

Albright Stonebridge Group (ASG), part of **Dentons Global Advisors,** is the premier global strategy and commercial diplomacy firm. As a multidisciplinary advisory firm, we help clients understand and successfully navigate the intersection of public, private, and social sectors in international markets. ASG's worldwide team has served clients in more than 120 countries.

For additional information or to arrange a follow-up, please contact Tomas Valdes, Director, Middle East & North Africa Practice.

Tomas Valdes
Director
Middle East & North Africa Practice
tvaldes@albrightstonebridge.com

Anarkalee Perera
Director
Technology Policy & Strategy Group
aperera@albrightstonebridge.com