April 9, 2024

Global Data Alliance Comments on
The Draft Data Sovereignty Public Policy of the Kingdom of Saudi Arabia

Submitted to the Saudi Data & AI Authority (SDAIA)

The Global Data Alliance (**GDA**)[1] welcomes the opportunity to submit comments to the Saudi Data & AI Authority (SDAIA) on its inquiry regarding the Draft Data Sovereignty Public Policy of the Kingdom of Saudi Arabia.[2]

The GDA is a cross-industry coalition of companies that are committed to high standards of data privacy and security and that rely on the ability to transfer data responsibly across borders to support jobs and economic growth. Alliance members are active across 15+ sectors and over 150 countries. The GDA advances policies that promote the responsible handling of data without imposing unnecessary data localization mandates or restrictions on data transfers.

The Draft Data Sovereignty Public Policy raises important considerations, including: (1) protecting the privacy of Individuals; and (2) safeguarding against illegitimate access or acquisition of data critical to national vital interests without the consent of competent authorities. We respectfully submit that Saudi Arabia should seek to protect these interests in ways that are compatible with other goals in the Draft Data Sovereignty Public Policy, which include: (3) accelerating digital transformation; (4) supporting innovation; (4) enabling the private sector; (5) creating a conducting business environment; and (6) attracting foreign direct investments in ways that aligned with economic sustainability and the national interest. We welcome SDAIA's recognition of the importance of "balancing data development, enablement, and governance" with national sovereignty.

We respectfully submit that SDAIA should avoid any recommendations to impose overbroad or unduly strict data localization or cross-border data restrictions. We acknowledge that some governments view narrow data transfer restrictions to be appropriate in very limited circumstances involving a clear and demonstrable risk to national security.

We urge SDAIA to avoid any broader application of such restrictions, which would undermine its other goals relating to privacy, digital transformation, the private sector, and foreign direct investment. We note, for example, the experience of the People's Republic of China, which imposed the world's most complex and onerous cross-border data policy framework – resulting in a sharp loss of foreign investor confidence, a worsening business environment, and reduced opportunities for digital transformation and private sector engagement. China is now trying to undo the negative impacts of its overly burdensome cross-border data policies. It is unclear whether China will be able to undo this damage.

Other economies – including India, Pakistan, the Philippines, and the EU – have also recently retreated from proposals to more strictly limit cross-border data transfers and to require strict data localization. These economies were persuaded to adopt a more reasonable approach by the overwhelming evidence of the harms that such restrictions impose on the countries that adopt them. We kindly encourage SDAIA to draw insights from the experience of these and other economies – such as Australia, Canada, Japan, and Singapore – that have benefited immensely from policies designed to foster cross-border data transfers.

It is also important to ensure that as an ambitious science- and information-driven nation, Saudi Arabia maintains seamless cross-border access to knowledge, information, data, and digital tools from trusted partners across world. This access is critical to myriad policy objectives, ranging from

technology-specific priorities such as digital transformation and cybersecurity threat management to broader national and societal priorities relating to the economy, environment, finance, health, human rights, safety, security, and tourism within Vision 2030.

The ability to transfer data across transnational digital networks is critical not only to maintaining and enhancing sovereign capability in Saudi Arabia, but also to other important Saudi Arabian policy objectives, including those relating to the protection of cybersecurity,[3] economic development,[4] environmental sustainability,[5] innovation/intellectual property,[6] private medical insurance, privacy/personal data protection,[7] regulatory compliance,[8] and small business promotion.[9] Please see Annex I for additional details on the importance of cross-border data in protecting Saudi Arabian cybersecurity.

The ability to transfer data across transnational digital networks is also critical to many Saudi governmental functions, including in relation to agriculture,[10] clean energy,[11] finance,[12] and health[13] / [14]. Finally, scientific and technological progress require the exchange of information and ideas across borders[15]: As the WTO has stated, "for data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies."[16] Please see Annex II for additional details on the importance of cross-border data in protecting other Saudi Arabian government priorities.

We hope that our comments will assist the SDAIA. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Joseph P. Whitlock

Executive Director
Global Data Alliance

Annex I

Importance of Cross-Border Data & Digital Trade to Saudi Arabian Cybersecurity

Cross-border data transfers are critical to cybersecurity in part because they allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Additionally, companies may choose to store data at geographically diverse locations to obscure the location of data and reduce risk of physical attacks, to enable companies to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location. Conversely, when governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities, as summarized below:

- **Data Transfers & Integrated Cybersecurity Planning.** Data transfer restrictions and localization requirements force organizations to adopt a siloed approach to data, often restricting the locus of certain data, but not others. This differentiation creates unnecessary technical complexity without any corresponding benefit to security. Simply put: artificial requirements to store data within borders strain the people, processes, and technologies an organization needs to manage its cybersecurity risk.

- **Data Transfers & Cybersecurity Awareness.** Data transfer restrictions and localization requirements impede visibility of cybersecurity risks, not only at the intra- and inter-organizational levels, but also at national and international levels. If cyber defenders cannot access threat indicators or other cybersecurity data collected in one jurisdiction, it becomes harder to address malicious cyber activity in other jurisdictions.

- **Data Transfers & Cybersecurity Collaboration.** Data transfer restrictions and localization requirements can impede cross-border collaboration, information sharing, and other coordinated network defense. When such restrictions and requirements isolate network defenders from each other, they cannot adopt a unified and coordinated defensive posture against malicious actors that do not respect national borders. In short, data transfer restrictions can give malicious actors that do not respect local legal requirements a lasting structural advantage over cyber defenders that do.

- **Data Transfers & Third-Party Cybersecurity Services.** Many organizations amplify their own cybersecurity risk management through third-party cybersecurity service providers. Best-in-class services depend on access to cyber data from around the globe. Without this access, these services and their users become more vulnerable to compromise.

- **Data Transfers & Cybersecurity Resiliency.** Whether a particular geographic area is at high risk for a natural disaster or in a potential future war zone, having data efficiently distributed is a crucial component of resiliency. The misconception that keeping data only within national boundaries will increase its security can actually create significantly more risk.

- **Data Transfers & Protectionism in the Name of Cybersecurity.** Localizing data within a country—or blocking its transfer—has no functional cybersecurity benefit. Security is determined by the technical and operational protections that accompany the data, not the location. Transfer restrictions and localization requirements are often used to advance other objectives. Perhaps the most systemic problem with using cybersecurity laws to require localization, then, is that it diminishes the role of laws and policies that are truly designed to improve security.

Annex II

Importance of Cross-Border Data & Digital Trade to Saudi Arabian Public Sector Priorities

Cross-border access to information and data transfers are critical for numerous objections, operations, and functions of the Saudi Arabian government. This includes:

1. **Artificial Intelligence:** Meeting goals relating to AI research in vital areas like healthcare and climate change, which depend upon ensuring continued Saudi Arabian cross-border access to high quality data from around the world.

2. **Cyber- and Homeland Security**: Cyber-defenders cannot protect Saudi Arabian networks without cross-border access to global cyberthreat intelligence. Likewise, Saudi Arabian border authorities depend upon cross-border digital access to international supply chain threat intelligence to interdict dangerous imports various border enforcement programs.

3. **Economy:** Saudi Arabian commercial and trade authorities depend upon cross-border access to information regarding business, sales, and export opportunities available to Saudi Arabian citizens.

4. **Environment**: Saudi Arabian environmental authorities depend upon cross-border access to satellite, meteorological, emissions, and other data from across the globe to advance efforts at combatting climate change and promoting a sustainable environment.

5. **Finance**: Saudi Arabian financial authorities depend on cross-border access to financial information flows to combat terrorist financing, money laundering, corruption and fraud. Securities and tax authorities also require ready cross-border access to financial information to fulfill their respective statutory functions.

6. **Foreign Policy**: Saudi Arabians Department of Foreign Affairs and Trade relies on cross-border data transfers for every aspect of its work in advancing Saudi Arabian foreign policy, interests, and security abroad. This extends to efforts to negotiate trade agreements, defend human rights, and promote foreign economic development.

   Health & Safety: Saudi Arabia's health authorities depend upon reliable cross-border access to health data in many contexts. This includes maintaining cross-border access to pre-clinical and clinical trial data from around the world to evaluate new treatments and healthcare solutions. It also includes real-time access to global epidemiological statistics and pandemic-related indicators to protect Saudi Arabia's population from emergent health risks. It also includes cross-border access to scientific publications and laboratory results from around the world to promote scientific advances, as well as cross-border access to pricing data for healthcare delivery purposes. The availability of new digital solutions enables healthcare providers to offer timely and effective interventions to patients and has given rise to a new face of health care, including mobile apps. Data sharing and integration are essential for creating a more connected and effective digital health ecosystem, as they facilitate better-informed decision-making, promote research and innovation, and enhance patient care.
7. **Private Medical Insurance:** As private medical insurance expands in Saudi Arabia as envisaged by Vision 2030, safe and secure technology platforms that have interoperability and permit cross-border transfer and data portability, is a key enabler for customers to access their health information within and across the sector.

8. **Innovation & IP:** IP-focused agencies in Saudi Arabia depend on cross-border access to data on inventions, creations, and R&D from abroad, including to assess prior art, registrability, and ownership of IP, as well as foundational research across the sciences.

[1] Global Data Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, electronics, entertainment, financial and payment services, health, consumer goods, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. For more information, please see www.globaldataalliance.org
[2] https://istitlaa.ncc.gov.sa/en/Transportation/NDMO/DataSovereigntyPolicy/Pages/default.aspx
[3] Global Data Alliance, *Cross-Border Data & Cybersecurity* (2023), https://globaldataalliance.org/issues/cybersecurity/
[4] Global Data Alliance, *Cross-Border Data & Economic Development* (2023), https://globaldataalliance.org/issues/economic-development/
[5] Global Data Alliance, *Cross-Border Data & Environmental Sustainability* (2023), https://globaldataalliance.org/issues/environmental-sustainability/
[6] Global Data Alliance, *Cross-Border Data & Innovation* (2023), https://globaldataalliance.org/issues/innovation/
[7] Global Data Alliance, *Cross-Border Data & Privacy* (2023), https://globaldataalliance.org/issues/privacy/
[8] Global Data Alliance, *Cross-Border Data & Regulatory Compliance* (2023), https://globaldataalliance.org/issues/regulatory-compliance/
[9] Global Data Alliance, *Cross-Border Data & Small Business* (2023), https://globaldataalliance.org/issues/small-businesses/
[10] Global Data Alliance, *Cross-Border Data & Agriculture* (2022), at: https://globaldataalliance.org/sectors/agriculture/
[11] Global Data Alliance, *Cross-Border Data & Energy* (2022), at: https://globaldataalliance.org/sectors/energy/
[12] Global Data Alliance, *Cross-Border Data & Finance* (2022), https://globaldataalliance.org/sectors/finance/
[13] Global Data Alliance, *Cross-Border Data & Medical Technologies* (2023), https://globaldataalliance.org/sectors/medical-technology/
[14] Global Data Alliance, *Cross-Border Data & Biopharmaceutical R&D* (2022), https://globaldataalliance.org/sectors/biopharmaceutical-rd/
[15] Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdtinnovation.pdf
[16] WTO, Government Policies to Promote Innovation in the Digital Age, 2020 World Trade Report (2020), at: https://www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20-0_e.pdf