April 30, 2024

Global Data Alliance Comments re the
Regulation on Personal Data Transfer outside the Kingdom of Saudi Arabia

The Global Data Alliance (GDA)[1] welcomes the opportunity to provide feedback to the Saudi Data and AI Authority (SDAIA) on the *Regulation on Personal Data Transfer outside the Kingdom* ("the Regulation"). This submission builds on the following GDA submissions to Saudi Arabia: (1) GDA Comments on Data Transfer Regulation (July 31, 2023); (2) GDA Comments on Data Sovereignty Public Policy (April 9, 2024); (3) GDA Comments on the Draft Executive Regulation on the Personal Data Protection Law (March 2022); (4) GDA Comments on the Revised Personal Data Protection Law (Sept. 2022); and (5) GDA Comments on the Draft Amendments to the Personal Data Protection Law (Dec. 2022).

The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The GDA supports policies that help instill trust in the digital economy without imposing undue cross-border data restrictions or localization requirements that undermine data security and economic development.

The GDA supports efforts in Saudi Arabia to develop a legal framework to protect individual privacy and personal data, while continuing to enable and facilitate the responsible transfer of data across transnational digital networks. We are grateful that Saudi Arabia engages so actively with the Saudi Arabian public and stakeholders from around the world on these issues. We also welcome any engagement by SDAIA in global cross-border data initiatives, including the Data Free Flow with Trust (DFFT) initiative and the Global Cross Border Privacy Rules (CBPR) Forum. This positive momentum will produce benefits in various cross-border data policy and international investment indices, such as the GDA Cross-Border Data Policy Index.[2]

At the same time, we observe with some regret that the 2024 draft Data Transfer Regulations have further diverged from international norms and best practices, as compared with the 2023 draft regulations. The current regulations no longer clearly reflect the tripartite framework (2023 draft regulations) that allowed for cross-border data transfers via any one of the following three mechanisms:

(1) Safeguards for transferring personal data (including binding common rules (BCRs), standard contractual clauses (SCCs), certification of compliance, and binding codes of conduct) [Art. 6];
(2) Exceptional cases where these safeguards are not applicable (including in cases in which the transfer is necessary for the performance of any agreement to which the data subject is a Party) [Art. 7]; and
(3) A system to determine the adequacy of each partner country's personal data protection frameworks according to norms detailed in the Regulation [Arts. 3-4].

In these April 2024 recommendations, we urge Saudi Arabia to return – to the greatest extent possible – to a framework that reflects all of these widely accepted cross-border data transfer mechanisms and international best practices.

Our comments and recommendations follow:

A. Predicating Data Transfers Upon on Article 3 Adequacy Determinations Will Undermine Both Privacy and Other Policy Priorities

The 2024 draft Data Transfer regulations place much greater emphasis on the Article 3 adequacy determination process and less emphasis on alternative transfer mechanisms (BCRs, SCCs, certifications, codes of conduct). We note that some of these references are now entirely omitted, while the scope of applicability of others has been narrowed. We urge SDAIA to reconsider this approach. Among other things, undue reliance on adequacy frameworks – to the exclusion of the other transfer mechanisms found in the EU's General Data Protection Regulation and other leading global privacy frameworks – will impose significant burdens on SDAIA and the Saudi government without any clear benefits. Adequacy determinations require significant investments in regulatory and administrative infrastructure as well as staffing almost exclusively on government acts. In contrast, the alternative transfer mechanisms (BCRs, SCCs, codes of conduct) are premised on shared responsibility with the private sector, whereby private sector entities would be accountable for ensuring the continued protection of the personal data of Saudi data subjects throughout the data transfer process. We respectfully submit that imposing these shared obligations on private sector entities – in line with international best practices – will produce superior privacy and data protection outcomes for Saudi Arabia than not doing so.

Over-reliance on Article 3 adequacy determinations may also create unintended consequences by making it more difficult for Saudi entities and individuals to communicate and conduct business with other countries. For example, if Saudi Arabia's major trading partners, including the United States or other economies across Europe, the Middle East, Africa, and Asia, are not quickly determined to meet Saudi Arabia's adequacy standards, and if alternative transfer mechanisms are not readily available, this could render it illegal for Saudi entities and individuals enterprises to engage in cross-border data transfers or to access digital tools, educational resources, or other information for their work, studies, and other needs. This would be an unfortunate and costly development. Millions of Saudi Arabian citizens, their families, and communities depend upon such access, as does the Kingdom and its government.

The ability to transfer data securely across transnational digital networks is of central importance to the national policy objectives of many countries, including Saudi Arabia. Data transfers support digital connectivity, cybersecurity, fraud prevention, anti-money laundering, and other activities relating to the protection of health, privacy, security, and regulatory compliance.

This ability also supports shared economic prosperity. Cross-border access to marketplaces, purchasers, suppliers, and other commercial partners allow Saudi enterprises in all sectors to engage in mutually beneficial international transactions with foreign enterprises. Data transfers, which are critical at every stage of the value chain for companies of all sizes, support global supply chains and promote productivity, safety, and environmental responsibility. This ability also supports scientific research and development across borders.

B. Permitting Data Transfers on the Basis of Adequacy Determinations and Other Transfer Mechanisms Will Advance Both Privacy and Other Policy Priorities

It is critical that Saudi Arabia's data transfer regulations reflect alternative transfers mechanisms – including BCRs, SCCs, codes of conduct, and certification mechanisms – for many reasons.

Broadly speaking, these mechanisms support the so-called "accountability principle," which is the prevailing international global norm that governs the relationship between personal data protection and cross-border data transfers. Under this norm, organizations that transfer data globally should implement procedures to ensure that data will continue to be protected, even if it is transferred to countries other than where it was first collected. The accountability principle was first developed by the OECD,[3] and was subsequently endorsed and has been integrated in many legal systems including the EU,[4] Japan,[5] New Zealand,[6] Singapore,[7] and Canada.[8] This principle is also a significant feature of the APEC Privacy Framework,[9] the

APEC Privacy Recognition for Processors (PRP) system,[10] the APEC Cross Border Privacy Rules (CBPR) system,[11] and the ASEAN Model Contractual Clauses.[12]

Different types of organizations and different business models require the use of different transfer mechanisms that are not interchangeable. In practice, larger companies will often rely on one or more data transfer mechanisms, using the tool most tailored to their business needs and to the specific data transfer(s) at hand. Other companies may principally rely only on one mechanism, such as adequacy determinations or standard contractual clauses. Creating a range of flexible transfer mechanisms that can be used differently in these different situations will help companies transfer data responsibly, consistent with Saudi Arabian law.

Data transfer mechanisms designed for use by companies operating in one country also cannot be viewed in isolation from mechanisms created and used in other countries. As countries worldwide develop and update their personal information protection laws and regulations it is critical that these legal frameworks are designed to effectively protect privacy in a manner that is internationally interoperable, flexible enough to account for rapid evolution in both technologies and business models, levels of risk, and that prioritizes high standards of data protection. This is particularly important in the context of international data transfers, where interoperable legal requirements support organizations' ability to comply with obligations across jurisdictions.

Of course, the context and perspective around privacy and personal data protection may appropriately vary among different countries based on cultural expectations, legal traditions, and other factors. At the same time, governments should support the common recognition of international norms and practices around core substantive protections that underpin interoperable privacy frameworks. If countries instead adopt fragmented policies on core issues, it undermines personal data protection and privacy, data and cybersecurity, and many other policy priorities.

C. Importance of Standard Contractual Clauses

We particularly urge Saudi Arabia to recognize that contractual transfer mechanisms from other jurisdictions or intergovernmental organizations may offer a workable model for contractual mechanisms that are consistent with Saudi Arabia's legal requirements. Many global companies have already adopted contract-based transfer mechanisms that protect data as it is transferred between countries and regions. We encourage Saudi Arabia to recognize that these existing contracts may already satisfy Saudi legal requirements – without requiring companies to re-negotiate those contracts to adopt unique, country-specific pre-approved language or formats. This approach to contractual transfer safeguards drives harmonization by recognizing alignment between these existing mechanisms and Saudi Arabian legal requirements – and ensures that companies can leverage existing compliance practices and mechanisms in support of products, services, and customers in Saudi Arabia.[13] In addition, participation in international certification systems can also advance convergence and interoperability.

GDA member companies have adopted contractual transfer mechanisms including the:

- European Union's Standard Contractual Clauses (EU SCCs);
- United Kingdom's International Data Transfer Agreements (UK IDTAs); and
- APEC Cross Border Privacy Rules System and the accompanying APEC Privacy Rules for Processors (APEC CBPRs and APEC PRPs)

We also recommend that Saudi Arabia prioritize flexibility in the appropriate format for standard contractual arrangements, including for existing contractual arrangements that already meet substantive obligations of Saudi Arabian law. For example, one interoperable approach that Saudi Arabia could consider to leveraging existing contractual mechanisms is to create a model addendum that can be added onto other contractual mechanisms, such as an addendum to the EU SCCs. The UK Information Commissioner's Office (UK ICO) recently adopted this approach in two new sets of model contractual clauses that came into force this year.[14]

The creation of such addenda – which recognize the substantive protections in the underlying contractual transfer mechanism and adopt a set of additional protections designed to satisfy the requirements of a second jurisdiction – helps support interoperability of data transfer mechanisms across jurisdictions.[15]

Finally, if Saudi Arabia adopts new model SCCs, we encourage Saudi Arabia to account for the range of different entities that transfer data and the range of different transfers between these entities. Any new contractual mechanism should support transfers between two controllers, from a controller to a processor, from a processor to a controller, or between processors.[16] Data transfers take many shapes and forms and it is important that contractual transfer mechanisms can be used in the full range of transfer scenarios. For example, the EU recently updated its SCCs to adopt a modular approach that organizations can use to support these different types of transfers. Whether Saudi Arabia adopts a modular approach or not, any new SCCs in Saudi Arabia should be flexible enough to be used in each of these scenarios.

D. Transfer of Sensitive Personal Data

Articles 4 and 7 of the data transfer regulations contain numerous restrictions on the cross-border transfer of sensitive data (i.e., prohibiting sensitive data transfers under SCCs, prohibiting sensitive data transfers in the case of scientific research, prohibiting sensitive data transfers even if those would benefit the data subject, and imposing special risk assessment requirements). We urge you to reconsider these restrictions, which will substantially isolate Saudi Arabia from interconnected, international healthcare research, delivery, and support systems.

Sensitive data sharing and integration are essential for creating a more connected and effective global health ecosystem, as they facilitate better-informed decision-making, promote research and innovation, and enhance patient care. 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. We would urge that the regulations be amended to remove the specific prohibitions in Articles 4, and instead to specifically permit the cross-border transfer of sensitive data.

E. Data Residency

The PDPL permits cross border data transfer under limited circumstances, but the implementing regulations and the law are unclear about whether data must reside in the Kingdom. We wanted to confirm whether with consent, data can be hosted outside the Kingdom or whether it needs to be hosted in the Kingdom but could be processed outside the Kingdom.

F. Risk Assessment Requirements Should be Carefully Designed

Article 7 imposes requirements to conduct risk assessments of transferring or disclosing personal data to an entity outside of Saudi Arabia. We would encourage SDAIA to make these risk assessments as reasonable and practical as possible. For example, under Article 7, data transfer risk assessments must include an assessment of undefined “material or moral impacts” of data transfers. We would recommend that Saudi Arabia clarify the scope of this provision, ensuring that it is not overly preclusive. We would assume “material impacts” to relate to the national defense of the Kingdom. Greater clarity – and appropriately narrow scoping – would promote the implementation and adoption of the regulations.

G. Studying the Experience of Other Economies May be Instructive

We also encourage SDAIA to study what has been successful – and not successful – in other economies around the world. 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.

H. Conclusion

In conclusion, we urge SDAIA to seek greater interoperability with other international data transfer regimes; to adopt a "shared responsibility" and "accountability" standard by aligning with SCCs, BCRs, certification mechanisms and codes of conduct that are widely accepted; to permit transfers of sensitive data; and to avoid data residency (i.e., data localization) mandates. Please do not hesitate to contact us with any questions at gdainfo@bsa.org

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] The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, financial services, health, media and entertainment, natural resources, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org/downloads/aboutgda.pdf

[2] GDA, Cross-Border Data Policy Index (2023), https://globaldataalliance.org/resource/cross-border-data-policy-index/

[3] OECD Privacy Framework 2013 (p15), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[4] Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[5] Act on the Protection of Personal Information, https://www.ppc.go.jp/en/legal/

[6] Privacy Act 2020, https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[7] Personal Data Protection Act 2012, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[8] Personal Information Protection and Electronic Documents Act fair information principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[9] APEC Privacy Framework, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[10] APEC Privacy Recognition for Processors, reference needed

[11] APEC Cross Border Privacy Rules system, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

[12] ASEAN Model Contractual Clauses (2021), at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf; *See also,* Singapore Personal Data Protection Commission, Guidance for Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows in Singapore (2022), at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Singapore-Guidance-for-Use-of-ASEAN-MCCs.pdf?la=en#:~:text=The%20ASEAN%20Model%20Contractual%20Clauses%20%28ASEAN%20MCCs%29%20are,parties%20that%20protects%20the%20data%20of%20data%20subjects.

[13] A touchstone of future regulatory efforts should be to seek to ensure interoperability between Saudi Arabian regulations and those of the EU, the USA and other jurisdictions. As Saudi Arabia considers the

possibility of new regulatory requirements, we encourage the establishment of reasonable grace periods and due respect for business predictability and legal certainty.

[14] *See* UK ICO, International Data Transfer Agreement and Guidance, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. First, the UK ICO adopted a 36-page standalone set of contract terms that companies could adopt to support transfers of data from the UK. Second, the UK ICO adopted a separate nine-page addendum, which companies can add to existing contracts that incorporate the EU SCCs; this allows companies to adopt the additional language in the addendum to support transfers of data from the UK. Adopting both a standalone set of SCCs and an addendum creates flexible options for companies transferring data from the UK, including for smaller businesses (which may not have other contractual mechanisms in place and thus may not make use of the addendum) and larger ones (which may already have existing contractual mechanisms that are readily modified by the addendum).

[15] We recommend ensuring that companies may seek to adhere by reference to a model addendum. Parties could provide that their contractual agreements incorporate the model addendum by reference, while noting that the agreement may provide for more specific terms on particular issues.

[16] We also note that in complex intercompany relationships, a particular entity may have different roles in different contexts, with respect to different information sets, and at different times, including as a controller, processor, importer, and/or exporter.