July 31, 2023

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

The Global Data Alliance (GDA)[1] welcomes the opportunity to provide feedback to the Kingdom of Saudi Arabia in relation to the *Regulation on Personal Data Transfer outside the Geographical Boundaries of the Kingdom* ("the Regulation"). This submission builds on the following GDA submissions to Saudi Arabia: (1) GDA Comments on the Draft Executive Regulation on the Personal Data Protection Law (March 2022); (2) GDA Comments on the Revised Personal Data Protection Law (Sept. 2022); and 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 Global Data Alliance supports policies that help instill trust in the digital economy without imposing undue cross-border data restrictions or localization requirements that undermine data security, innovation, economic development, and international trade.

The GDA congratulates Saudi Arabia on its progress towards developing a legal framework to protect personal data, while continuing to enable and facilitate the responsible transfer of data across transnational digital networks. Among other things, we welcome the decision by Saudi Arabia to allow for a tripartite framework that allows for cross-border data transfers via any one of the following three mechanisms:

(1) Safeguards for transferring personal data (including binding common rules, standard contractual clauses, 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].

Our recommendations focus on:

(1) Promoting convergence and interoperability among contractual transfer mechanisms with similar contractual transfer mechanisms in other jurisdictions;
(2) Clarifying several ambiguities and other important concepts that have not yet been addressed in the Regulation; and
(3) Addressing potential legal conflicts between the Regulation and other cross-border data measures in Saudi Law.

A. Introduction

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, innovation economic development, and international trade. Alliance member companies are significant investors in Saudi Arabia, collectively employing thousands of Saudi Arabian citizens and working to advance growth, innovation, and cross-sectoral diversification in Saudi Arabia.

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 COVID-19 recovery, 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.

We welcome the Regulation's recognition of the importance of cross-border data transfers and its adoption of several alternative mechanisms to allow for responsible and accountable data transfers.

B. Promoting convergence and interoperability among contractual transfer mechanisms

We commend the inclusion in Articles 3, 6 and 7 of data transfer mechanisms that have become a key instrument for both protecting data subjects' rights and for the development of the digital economy and international trade. More specifically, we welcome the Regulation's reflection of not only adequacy determinations (Article 3), but also standard contractual clauses, binding common rules, certification mechanisms, and other codes of conduct (Article 6), and mechanisms to permit transfers in other exceptional cases (Article 7).

We recommend Saudi Arabia promote convergence and interoperability of data transfer mechanisms with those established in other prevailing data protection frameworks, particularly in relation to standard contractual clauses.

Broadly speaking, the Article 6 and 7 mechanisms are especially welcome because they appear to comport with 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,[2] and was subsequently endorsed and has been integrated in many legal systems including the EU,[3] Japan,[4] New Zealand,[5] Singapore,[6] and Canada.[7] This principle is also a significant feature of the APEC Privacy Framework,[8] the APEC Privacy Recognition for Processors (PRP) system,[9] the APEC Cross Border Privacy Rules (CBPR) system,[10] and the ASEAN Model Contractual Clauses.[11]

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 raises the cost of business for all companies and can undermine personal data protection and consumer privacy.

Companies that provide services in more than one country must identify – and implement – additional privacy and data protection requirements imposed by each country in which they operate, keeping in mind how those obligations relate to regulations in other countries. Laws and regulations that promote convergence around internationally-recognized approaches to data transfers can help drive interoperable data transfer mechanisms, allowing companies to leverage these common approaches. In practice, a new transfer mechanism should be sufficiently similar – in structure and substantive protections – so that obligations under the new mechanism can be mapped onto obligations under the old mechanism. This ensures companies can understand how their obligations change across jurisdictions and allows them to identify shared requirements across legal frameworks. That approach creates a more efficient compliance process and drives investment in strong practices that companies can leverage in more than one jurisdiction. There is an important role for policymakers in fostering such interoperable approaches to data transfers.

C. Clarifying several ambiguities and other key concepts

As Saudi Arabia progresses in finalizing and implementing the Regulation, we recommend that it clarify several potential ambiguities or other important concepts, as set forth below.

1. Design of Standard Contractual Clauses

The Regulation contains a detailed description of binding common rules, but not of standard contractual clauses. We 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.[12] 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.[13] 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.[14]

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.[15] 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.

2. Transfer of Sensitive Personal Data

The regulations provide extensive guidance for the transfer of personal data outside the Kingdom but appear to be silent on the cross-border transfer of sensitive data. 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. 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 specifically permit the cross-border transfer of sensitive data.

3. 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.

4. Vital Interests of Saudi Arabia

Under Articles 2, 8, and 9, the operation of key provisions in the Regulation could be rendered inutile if they are seen to implication the "Vital Interests of the Kingdom." We would recommend that Saudi Arabia clarify the scope of this provision, which we would assume to relate to the national defense of the Kingdom (among other topics). To provide legal certainty regarding the operation of Articles 2, 8, and 9 (among other articles), it would be helpful to include a cross-reference to other measures that define "Vital Interests of the Kingdom" or otherwise specify what these are.

D. Addressing Potential Legal Conflicts between the Regulation and Other Cross-Border Data Measures in Saudi Arabia

There remain in other Saudi legal measures several other data localization requirements or data transfer restrictions,[16] as reflected in Saudi Arabia's ranking as a highly restrictive jurisdiction in the GDA Cross-Border Data Policy Index.[17] Article 2 of the Regulation would allow these measures to continue to coexist and apply alongside the data transfer mechanisms in the Regulation.[18] This approach creates a potential legal conflict.

The continuing application of the cross-border data restrictions in measures raise fundamental questions about the applicability of the data transfer mechanisms in the Regulation, and could render those transfer mechanisms inutile under some legal interpretations. We urge Saudi Arabia to include clarifying language in the final Regulation that will provide legal certainty that the Regulation supersedes conflicting prior cross-border data restrictions. It is necessary to address these apparent conflicts of law in order to provide confidence (to governmental and private stakeholders alike) that it is indeed legally permissible to use the Regulation's data transfer mechanisms.

* * *

Thank you again for your focus on promoting interoperable mechanisms to support international data transfers. We welcome an opportunity to further engage with Saudi Arabia on these important issues.

---

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

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

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

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

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

[7] 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/

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

[9] APEC Privacy Recognition for Processors, reference needed

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

[11] 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.

[12] 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.

[13] *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).

[14] 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.

[15] 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.

[16] Other data localization requirements and data transfer restrictions may be found in the following measures:

Saudi Arabia Communications & Information Technology Commission, *Cloud Computing Regulatory Framework* (published Feb. 6, 2018, effective March 8, 2018), https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf (Art. 3-3-8: The cloud computing service providers registered with CITC and cloud computing subscribers shall not transfer any content from the Saudi Government Data outside the Kingdom for any purposes, or in any form, whether permanently or temporarily (for example: temporary storage and backup, or similar purposes), unless it is expressly stated that it is permitted according to the laws or regulations in the Kingdom, except for this "Regulatory Framework." Art. 3-3-10: Without prejudice to their obligations stipulated in Article 3-3-7, CSPs registered with CITC must clearly inform CITC and the Cloud Subscriber in advance and get their approval, if the cloud subscribers' content will be transferred, stored, or processed outside the Kingdom, permanently or temporarily)

Saudi Arabia National Cybersecurity Authority, Essential Cybersecurity Controls (ECC-1:2018), https://itig-iraq.iq/wp-content/uploads/2019/08/Essential-Cybersecurity-Controls-2018.pdf (*See* Art. 4-1-3-2: "With respect to at KSA government organizations, as well as private sector organizations owning, operating, or hosting Critical National Infrastructures, any "cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.";

DRAFT Cloud Cybersecurity Controls (CCC-1: 2020) (to modify/extend ECC: 1 2018) (issued Feb. 2020), https://www.tamimi.com/law-update-articles/saudi-arabias-draft-cloud-cybersecurity-controls/

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

[18] The Article 2 provisions at issue are as follows:

(1) The provisions of this Regulation shall not prejudice the provisions of the applicable laws in the Kingdom or the conventions to which the Kingdom is a party…
(3) Subject to the provisions of the Law and its Regulations, a Controller may Transfer Personal Data or disclose it to a party outside the Kingdom, provided that such Transfer or Disclosure does not impact the national security or the Vital Interests of the Kingdom or violate any other law in the Kingdom.

(emphasis added).