Whitepaper on Regulatory Implications for Cross-Border Data Transfers from Saudi Arabia to the United States

Prepared by Sia Partners as of June 2018

Table of Contents

I. Scope

This whitepaper summarizes privacy requirements related to the cross-border transfer of data from the Kingdom of Saudi Arabia ("Saudi Arabia") to the United States of America ("US"). Using research conducted in April 2018 with the assistance of a global law firm, this paper outlines the following regulatory compliance scenario: *a Saudi Arabia-based financial institution transfers* ***Financial and/or Customer Data*** *cross-border to a US service provider.* The structure of this transfer could be one where the financial institution either (a) outsources its information directly cross-border to the US service provider, or (b) stores the data on the cloud, where a US service provider would then source the data. Key considerations include Saudi Arabian data privacy laws on banks and financial institutions, requirements related to methods of transferring **Financial and/or Customer Data** and best practices.

II. Executive Summary

While Saudi Arabia has principles in place relating to the general protection of an individual's privacy, there is currently no dedicated legislation concerning data protection. A number of regulations, which do exist, apply to financial institutions with regard to transfers of **Financial and/or Customer Data**. These are specific to the Capital Markets Authority ("CMA") of Saudi Arabia responsible for regulating, supervising and developing capital markets activity in Saudi Arabia, and the Saudi Arabian Monetary Authority ("SAMA"), and consist of various regulations designed around having a general duty of confidentiality and relate to the privacy and safeguarding of customer data. Accordingly, the requirements focus on the restrictions related to the outsourcing, disclosure and transfer of customer data abroad (subject to limited exceptions). Although the prior written consent from data subjects (i.e., customers) has not yet been expressly required, disclosures (i.e., approval/no objection) related to the functions to be outsourced (i.e., processing, transmission or retention of customer or financial data) are required by governmental authorities such as SAMA prior to data transfer.

Additionally, cloud computing service providers face a number of restrictions based on the types of customer content to be stored or processed as defined in the Cloud Computing Regulatory Framework ("CCRF"), which was issued in early 2018 by the Communications and Information Technology Commission ("CITC"). Therefore, having a comprehensive understanding of the proposed cloud infrastructure is important.

Although the rules currently only apply to, and are enforced on, banks and financial institutions, they will likely require service providers receiving the outsourced data to comply with confidential data obligations.

III. Background

Although Saudi Arabia does not currently have dedicated data protection legislation,[i] Sharia (or Islamic) principles do exist for the general protection of an individual's privacy. Because the operating model of a service provider, in this case, would be to store applicable data, run corresponding calculations and execute certain business processes within the US, any entity holding confidential, private or personal data would be advised to obtain prior written consent from their data subjects with respect to processing, using or transferring the **Financial and/or Customer Data** cross-border to the US.

There are a number of secular regulations in place related to banking and insurance that are distinguished by the method of data transfer, as well as by the type of financial institution (i.e., banks, insurance, "authorized persons" conducting financial business, etc.). These are regulated by the following government authorities and apply when transferring data cross-border from Saudi Arabia:

- The Saudi Arabian Monetary Authority ("SAMA") is the central bank of the Kingdom of Saudi Arabia responsible for oversight of financial institutions in Saudi Arabia, which includes imposing disclosures of confidential information and issue approvals/no-objections to data transfers where appropriate.
    - ***SAMA Rules on Outsourcing, July 2018***
    - ***SAMA, Finance Companies Control Law and its Implementing Regulations***
    - ***SAMA, Finance Companies' Consumer Protection Principles, June 2015***
    - ***Banking Consumer Protection Principles, June 2013 (The BCPP has been issued by the Consumer Protection Department of SAMA)***
- The Capital Markets Authority of Saudi Arabia ("CMA") is responsible for regulating and developing the Saudi Arabian Capital Market by issuing required rules and regulations for implementing the provisions of Capital Market Law:
    - ***The Capital Market Law, Royal Decree No. M/30 dated 2/6/1424H***
    - ***CMA Merger and Acquisition Regulations, Issued by the Board of the CMA pursuant to Resolution Number 2-94-2017, dated 25/1/1439H***
- The BCL regulates banking businesses and includes requirements relating to banking business and activities.
    - ***Banking Control Law No. M/5 dated 22/2/1386 H, corresponding to 11 June 1966***
- The ICPP imposes obligations related to data protection and confidentiality with respect to insurance companies and insurance related service providers.
    - ***Insurance Consumer Protection Principles, July 2014***
    - ***Insurance Market Code of Conduct Regulation***
- The Communications and Information Technology Commission issued a Cloud Computing Regulatory Framework ("CCRF") in early 2018, which includes provisions that apply to any "cloud service" provided to cloud customers having a residence or customer address in Saudi Arabia.
    - ***Cloud Computing Regulatory Framework***

In addition, the common objective of these regulations is to oversee how financial institutions safeguard and transfer data in relation to conducting banking business. Generally, any cross-border transfer of data should not cause detriment or harm to the owners of that data. For example, Saudi Arabia requires that banks and financial institutions adhere to the following requirements:

- Protect consumer data and maintain its confidentiality, including while held by a third party (such as a service provider based in the US);
- Provide a safe and confidential environment in the delivery channels to ensure the confidentiality and privacy of consumer data;
- Maintain procedures, system controls and employee awareness to protect consumer information and identify and resolve security breaches; and
- Ensure data is only accessed by authorized personnel.

It is important to note however, that while banks have a general duty of confidentiality towards customer data, exceptions apply when the disclosure is being imposed by a regulatory body (i.e., Ministry of Interior, court mandated) or when the disclosure is made by written consent by the customer.

IV. Outsourcing Rules

Prior to a Saudi Arabian bank or financial institution outsourcing **Financial and/or Customer Data** to a service provider (i.e., third party) for the purposes of using that information for its business, it must first comply with the outsourcing rules. "Outsourcing"[ii] rules apply to all cross-border outsourcing arrangements involving **Financial and/or Customer Data** between Saudi Arabian-based financial institutions and service providers. The objective of SAMA's outsourcing rules is to regulate financial institutions outsourcing functions involving **Financial and/or Customer Data** to service providers because cross-border data transfers gives rise to heightened exposure of additional risks.

Generally, SAMA imposes the following data and confidentiality requirements on banks and financial institutions:

- SAMA approval/no-objection prior to outsourcing **Financial Data**[iii];
- Proposed outsourcing arrangement complies with relevant statutory requirements related to customer confidentiality;
- Certain functions cannot be outsourced to a Service Provider, including: transmissions, processing and retention of **Customer Data**[iv] other than for credit card processing and remittances utilizing international payments systems; and
- Retrieve customer data upon termination of the relationship, and report to SAMA all instances where the retrieval was not considered successful.

In order to receive the approval/no-objection from SAMA, the bank or financial institution must provide the government authority with certain information prior to transferring the **Financial and/or Customer Data** to the service provider. Because this scenario describes transferring **Financial Data**, the bank or financial institution must describe/supply the following to accompany its request to SAMA:

- Functions/processes being outsourced (i.e., capital calculations, storage, processing);
- Categorization of whether the outsourcing is "material;"[v]
- Rationale for the outsourcing;
- Details on the overseas service provider;
- Nature and disposal of the data to be transferred;
- Legal opinion on compliance with Saudi Arabian laws and regulations;
- Provide SAMA access to data related to "material" outsourcing if applicable, such as via business premises of service providers;
- Legal opinion confirming SAMA's access to the outsourcing activity at the service provider.

There are also a number of other requirements imposed on banks and financial institutions as part of outsourcing, which include being able to:

- Reach legally binding agreements with the third party;
- Notify breaches and legal requirements; and
- Perform a risk assessment depending on the nature of the outsourcing.

Saudi Arabian law and regulation **does not require data encryption** prior to cross-border transfer. Although banks, financial institutions, and other entities, must take necessary steps to safeguard the confidentiality of **Financial and/or Customer Data**, it is not currently mandated for them to use encryption technology.

V. Cloud Computing Service Providers

The Cloud Computing Regulatory Framework ("CCRF") applies to all "cloud services" provided to cloud customers (i.e., through cloud computing) having an address in Saudi Arabia. A "cloud service" includes information and communications technology services provided through "cloud computing,"[vi] offering storage, transfer or processing of customer content / data in a cloud system. Within the context of the CCRF, storage of customer information and performing IT "Big Data" solutions or analytics that rely on cloud computing solutions is not considered a "cloud service." However, for service providers offering scalable self-provisioning and administration on demand, the cloud computing service would likely be considered a "cloud service." From this definition, the physical presence of the service provider is irrelevant.

In the event that a service provider intends to perform any "cloud services," it must comply with the following requirements:

1. Register with the CITC a list of all individuals who would be responsible to exercise control (i.e., direct or effective) over data centers or other "critical cloud system infrastructure" hosted in Saudi Arabia for the purposes of cloud services, or would be involved in the processing and/or storage of customer content based on pre-defined levels, as follows:
    a. Level 1 content consists of non-sensitive customer content (i.e., individual customers or private sector companies not already subject to any sector-specific restrictions related to the outsourcing of data);
    b. Level 2 content consists of sensitive customer content (i.e., individual customers or private sector companies/organizations not subject to any sector-specific restrictions on the outsourcing of data);
    c. Level 3 content consists of customer content from private sector-regulated industries, including banking; and
    d. Level 4 content consists of highly sensitive or "secret" customer content belonging to the governmental authorities.

Under CITC guidelines, it is likely that **Financial and/or Customer Data** stored at banking and financial institutions would be categorized as Level 3 content and therefore, could only be transferred outside of Saudi Arabia if the service provider registers with the CITC.

VI. Questions Arising Related to Data Transfer

- ***Can position data originating from Saudi Arabia be held offsite/offshore (in the US)?***
- ***Can a full sub-ledger of details from Saudi Arabia be held offsite/offshore (in the US) with journal entry into the primary system?***
- ***Can capital calculations be outsourced (e.g. outside of the jurisdiction to the US)?***
- ***Can capital calculations relating to Saudi Arabia be performed offsite/offshore (in the US) (please identify what activities are going to be including in capital calculations)?***
- ***Can payment or asset transfer instructions be sent from offsite/offshore (outside the US) system to onshore systems (inside the US)?***
- ***What customer data originating in Saudi Arabia can be held offsite/offshore (in the US)?***

All of these questions can be answered with a *conditional* Yes. Consideration would need to be given to the type of third party activity that would take place (i.e., transfer of data or cloud computing) and to ensure that based on that, all of the necessary requirements have been met relating to the Saudi Arabian laws and regulations surrounding data privacy as it relates to **Financial and/or Customer Data**. If SAMA and the customer approves of the data transfer, then it can legally proceed. However, it would be advisable, albeit not required by SAMA, to have the counterparties agree in writing to (a) be compliant with relevant local laws, (b) obtain the necessary consents and approvals regarding the transfer of data to the US, and (c) indemnify the counterparty to cover any losses arising from breaching these obligations.

VII. Conclusion

Based on the scenario outlined in this whitepaper, banks and financial institutions in Saudi Arabia will likely require US-based service providers to comply with certain confidentiality obligations, despite the absence of dedicated legislation. The principles governing data transfers, as well as SAMA's key confidentiality restrictions on banks and financial institutions outsourcing, disclosing and transferring data to the US, will involve service providers being responsible for safeguarding, and preventing disclosure of **Financial and/or Customer Data** without either written consent from the customer or disclosure as imposed by a Saudi Arabian authority. Banks and financial institutions must also obtain prior SAMA approval/no-objection in relation to the outsourcing of any functions relating to the processing, transmission or retention of **Financial and/or Customer Data.**

In addition to the above requirements, there are best practices that should be followed prior to transferring Financial and Customer Data either cross-border or to the cloud by US-based service providers. These include obtaining written consent from the data's owners, reporting all data breaches to SAMA, and tailoring contracts between financial institutions and service providers. Such provisions include representations that both counterparties are compliant with relevant laws of Saudi Arabia and fulfilled all requirements (i.e., written consent from data owner) to transfer data to the US service provider, and to have an indemnity contract covering counterparty loss.

---

[i] A draft law related to freedom of information and protection of private data has been proposed and under by the Shura Council of Saudi Arabia for approximately two years.

[ii] "Outsourcing" is defined as an arrangement regarding a third party, such as a service provider, performing a previously carried out or new service to be launched by a financial institution.

[iii] "Financial Data" includes books of accounts, general and sub-ledger, financial statements, and various financial data other than Customer Data.

[iv] "Customer Data" is defined as any information or document that relates to the affairs or account of a customer, despite whether it is held physical or electronically, or whether the custodian is a financial institution or service provider.

[v] Additional obligations apply to "material" outsourcing. Some examples of functions when performed by a service provider that are **NOT** considered material include market information services, advisory, and independent consulting. It should be noted that financial data is considered to be "material" outsourcing.

[vi] "Cloud computing" is defined as the use of a scalable and elastic pool of shareable physical or virtual resources (such as servers, operating systems, networks, software, applications, and storage equipment) with self-service provision and administration on-demand.