BRACEWELL

INSIGHTS

Updates to Saudi Arabia's Data Protection Law

November 2, 2021

*By: **Christopher R. Williams** and **Amelia Bowring***

Whilst European and North American businesses are well accustomed to dealing with complex data protection legislation, businesses in the MENA region have by and large not had to consider the same in their local markets.

From a Saudi standpoint, the recently published Personal Data Protection Law (published on 24 September 2021 and effective as of 23 March 2022 ("**Effective Date**")) ("**PDPL**") changes this, imposing national regulation of data protection on companies across the Kingdom.

Data controllers in KSA have one year from the Effective Date, to comply with the provisions of the PDPL and such executive regulations that might be implemented going forward. In this note we consider how companies required to comply with the PDPL, including both companies doing business within KSA and companies outside KSA that process the personal data of Saudi residents, can prepare for the PDPL ahead of its implementation and in particular how the PDPL interfaces with existing legislation such as the Personal Data Protection Interim Regulations (" **PDPIR**").

KSA Company Data Protection Compliance Checklist

Ahead of the Effective Date, KSA companies should be looking to develop a data protection framework which is fully compliant with the PDPIR, which in turn will significantly assist future compliance with the PDPL, once in force. In order to do so, KSA companies should undertake the following actions:

1. **Training**: all employees should undergo a high level training programme, under which they learn and appreciate key data protection issues and risks associated with breaches. As all employees are likely to be handling personal data in some form, training of employees is absolutely imperative - this is an area that Bracewell can assist, in respect of the provision of in-house training and the like and have been doing so for companies subject to EU and US data protection laws.

2. **Data mapping exercise**: companies should identify the following information, namely: (i) what personal data is collected, processed, stored and transferred (as the case may be); (ii) what is the origin of such data; (iii) why such data is collected; and (iv) where such

data is stored, how is it transferred and to whom is it disclosed. The Annex to the new EU SCCs require companies transferring data outside the EU to provide most of this information, with the exception of where data is stored.

3. **Record keeping**: consider the manner in which data records are maintained and in turn comply with regulations going forward.

4. **Contract reviews**: all company contracts should be reviewed to identify gaps in data protection clauses and non-compliance. Any such gaps should be filled by way of amendments to such contracts, insofar as possible and particularly so for companies which also have access to EU data.

5. **Technology reviews**: all technology that is used to protect data should be reviewed for efficiency and to ensure it can deliver to the standards prescribed by the regulations.

6. **Cyber-attack response processes**: whilst not a requirement under the regulations, with the increasing number of cyber-attacks across businesses, during a review of a company's data protection functions it would be timely to develop a tested action plan to respond to any cyber-attacks on the organisation's systems. This is another area that Bracewell can assist and Bracewell have been doing so for clients across the globe in respect of their cyber-attack response processes.

7. **Consent language and purpose of data use**: ensure the organisation has a process in place to allow consenting to the collection and use of data, and ensure that systems are in place to maintain and store such consents and that the collection of data for relevant purposes are always appropriate and necessary.

8. **Data protection policies**: review existing policies, identify any gaps and consolidate policies encompassing obligations on the company, data providers' rights and the company's approach to personal data management. This is an area that Bracewell also currently assists clients with across the globe.

Key Issues to Consider for Compliance

The following is a list of key issues the PDPL covers and should be considered when looking at the compliance checklist:

Scope of the PDPL

The PDPL applies to the processing of individual personal data collected in KSA. It also captures data processing that occurs extraterritorially. Where Saudi businesses have a foreign data controller, a Saudi representative must be appointed and licensed by the Saudi Data and AI

Authority ("**SDAIA**") to perform PDPL data controller obligations. Uniquely, the PDPL's scope includes the processing of deceased persons' data.

Consent is Key

Having the data provider's consent is the primary basis for lawful processing and the (not-yet-published) executive regulations are expected to outline specific cases whereby consent must be in writing, alluding to circumstances where non-written consent may suffice. The PDPL allows for processing without consent where: (i) a "definite interest" is achieved of the data provider and they cannot be contacted; (ii) processing is in accordance with another law or the implementation of a preceding agreement and; (iii) the controller is a public entity and processing is required for security purposes to meet certain requirements.

Approval of Data Transfers

The PDPL provides for tight restrictions on data transfers outside of KSA which may only be done in the following situations: (i) necessity to preserve an individual's health or life; (ii) combatting disease; (iii) the disclosing party is satisfying an obligation by way of the transfer; (iv) it serves the Kingdom's interests or; (v) for other purposes yet to be identified by the executive regulations.

Transfers must also: (i) not prejudice national security; (ii) have guarantees preserving the confidentiality of the data that are no less standards than that of the PDPL; (iii) ensure personal data disclosure is limited to that which is absolutely necessary for the purpose and; (iv) ensure that the competent authority approves the transfer/disclosure, as to be determined by the executive regulations.

Notably, this approval requirement goes much further than the GDPR or U.S. states' transfer restrictions and makes the PDPL look more similar to ***China's new data protection law***, the PIPL.

Additional Controls

The PDPL states that the executive regulations will include additional restrictions for certain specific data. For health data, additional controls must be in place such as: (i) placing restrictions on access to such data and limiting to as minimum number of employees as possible for the purpose and; (ii) limiting health data processing procedures to the minimum number of employees as necessary for health insurance services purposes.

For credit card data, there must be necessary actions in place to verify the availability of written consent of the data provider, any change of the purpose of the collection of the data and its disclosure.

Marketing of Data

Data controllers are prohibited from using personal data for marketing, such as using individual information like postal or email addresses to send promotions without first obtaining consent and providing an opportunity to opt out.

Prohibition on Photocopying official documents

This common practice has been prohibited under the PDPL unless for the purposes of implementing its provisions or if a competent authority specifically requests it.

Registration Requirements

All data controllers must register with SDAIA who will charge a fixed fee for doing so under the (yet-to-be-published) executive regulations.

Additionally, records must be registered with SDAIA and any amendments thereto from time to time.

Individual Rights

Like China's new PIPL, GDPR, and state data protection laws in the U.S. like Virginia's Consumer Data Protection Act and California's new California Privacy Rights Act, the PDPL grants individuals rights regarding their own personal data, including the rights to access, rectification, and destruction/deletion. Additionally, the PDPL grants individuals the right to be informed, which requires processors to inform individuals as to the legal or practical justification and purpose for collecting their personal data.

Outlook

Saudi Arabia is taking a progressionist approach to national regulation of KSA companies' use of personal data in the Kingdom and, whilst the obligations mentioned above are more onerous than those currently in circulation, the grace period provided to Saudi companies to get their systems in place to comply with the PDPL, provides a welcome opportunity for internal data protection review and implementation of updates thereto. While this progressionist approach differs from the faster pace of China's new PIPL, unlike GDPR and U.S. state laws, violations of both the China's PIPL and the Kingdom's PDPL can trigger criminal penalties. Penalties for non-compliance are relatively severe, including up to one year imprisonment and/or a SAR 1 million (circa. USD 250,000) fine for unlawfully transferring data out of the Kingdom and up to two years imprisonment and/or a SAR 3 million fine (circa. USD 800,000) for disclosing sensitive data, as well as SDAIA's ability to impose fines up to SAR 5 million (circa. USD 1.3 million). Given the nature of such penalties it is in the interest of all businesses to ensure that the collection, use, storage and subsequent transfer of data is done in full conformance with data protection legislation.