An overview of Saudi Arabia's new Personal Data Protection Law

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data - Riyadh

Saudi Arabia's new Personal Data Protection Law Royal Decree M/19 of 9/2/1443H (16 September 2021); Cabinet Resolution No. 98 of 7/2/1443H (14 September 2021) has now been published in the Official Gazette, triggering a 180 day period, after which the Law will come into effect on 23 March 2022. Data controllers may have a year from that date, during which time they must modify their arrangements to ensure compliance.

While further detail will be set out in the associated Regulations, the Law seems to be a significant step in the right direction. In this note, we provide a general overview of the Law, along with some observations on areas that have potential to become pinch points.

Application

In this note, we have not sought to provide a detailed review of the terms defined in the Law. Some of these require further scrutiny, although in very general terms they do not seem to be far removed from the corresponding terms as used in other data protection laws.

With the exception of personal data processing for personal or domestic purposes, the Law applies to all personal data processing undertaken in Saudi Arabia, extending to personal data processing undertaken outside Saudi Arabia in respect of data subjects in Saudi Arabia. Personal data processing in respect of deceased persons is also within the scope of the law, if such processing could lead to the identification of that person or his or her family.

The Law is to be read subject to any other law or treaty that better protects personal data. We understand this to mean, if any other specific provisions of other Saudi laws, or treaties to which Saudi Arabia is a signatory, provide for stronger protection of personal data, then such stricter requirements will prevail. At a practical level, it is difficult to know what this will look like.

The Law is without prejudice to the authority of the National Cybersecurity Authority ("**NCA**") in respect of the cybersecurity subject matter for which it is responsible. It is unclear whether this is to be understood broadly, or whether it will be qualified in any way.

For the first two years, the 'competent authority' responsible for the implementation of the Law will be the Saudi Data & Artificial Intelligence Authority ("**SDAIA**"). The supervisory function will eventually shift to the National Data Management Authority ("**NDMO**"), which falls under SDAIA, as the data protection landscape develops. Different licensing authorities may be delegated responsibility for the functions of the competent authority in respect of entities in the industry sectors for which they are responsible, although this is unclear.

As the competent authority, SDAIA is required to issue the Regulations prior to the Law coming into effect in March 2022. The Regulations will be developed in consultation with various government entities, including the Ministry of Communications & Information Technology, the Ministry of Foreign Affairs, the Communications & Information Technology Commission ("**CITC**", the Saudi telecoms regulator), the NCA, the Central Bank ("**SAMA**"), and the Saudi Health Council.

The Law establishes a requirement for entities outside Saudi Arabia, that are processing personal data of

data subjects in Saudi Arabia, to appoint a representative in Saudi Arabia to fulfil their obligations under the Law and Regulations. There is a long-stop date (five years from the law coming into effect), by which time the head of the competent authority must implement this requirement.

The competent authority is expected to educate data subjects, as well as personnel in data controller entities, with respect to rights and obligations set forth in the Law. Data controllers will need to hold workshops for personnel in order to train them on concepts and principles found in the Law, and the competent authority may be called on to provide support in this regard.

Principles

The Law prohibits the processing of personal data without the consent of the data subject, except in specific circumstances. Consent is also required where the data controller wishes to process personal data for purposes other than those for which consent was originally obtained. The Regulations will provide further detail in respect of consent, including information on circumstances where consent must be obtained in writing, the ability of the data subject to withdraw consent at any time, and information on obtaining consent from those without legal capacity (such as minors). Consent is not to be a prerequisite for providing a service or benefit unrelated to the service or benefit in respect of which consent is sought / obtained.

The exceptions to the requirement for consent, as set out in the Law, may be summarised as follows:

- When the processing activity is in the interest of the data subject, and it is impossible or difficult to contact him or her;
- When the processing activity is carried out pursuant to another law, or to implement a prior agreement to which the data subject is a party; and
- When the data controller is a public entity and the contemplated processing is required for national security or the administration of justice.

Some of these exceptions seem familiar, relative to the approaches taken elsewhere. Others seem to be broad, and could be subject to abuse in terms of the discretion available to the data controller.

Generally, personal data may only be collected directly from data subjects, and processed only for the purposes for which it was collected. There are exceptions to this, enabling the processing of personal data collected other than directly from data subjects in certain circumstances. Further detail will be provided in the Regulations, although these exceptions include:

- With the consent of the data subject;
- If the personal data is collected from a publicly available source;
- When the data controller is a public entity and the contemplated processing is required for national security or the administration of justice;
- If following this requirement may harm the vital interests of the data subject;
- If collecting or processing the personal data is necessary for protecting the public health or the life or health of an individual or specific individuals; and
- If the personal data will be stored in a format that makes it impossible to identify the data subject.

Personal data may only be processed for lawful purposes, and the means of collecting and processing personal data need to be appropriate to the circumstances, bearing in mind the nature of the data subject, and the need for clarity and absence of deception.

There is a requirement for data minimisation, so that only the minimum personal data necessary for the contemplated purposes is collected and processed. Similarly, there is limitation requirement, whereby data controllers may retain personal data only for as long as is necessary to fulfil the purposes for which the data was collected. If personal data is no longer required, then it must be destroyed.

Besides considerations specific to sensitive data, the Law also provides specific considerations relative to certain types of sensitive data. Specifically, the Law contains particular restrictions applicable to health data and to credit information.

Data Subject Rights

The following data subject rights are available under the Law, subject to limitations that may be specified in the Regulations, or that may otherwise apply pursuant to the Law:

- The right to be informed of the legal basis for contemplated personal data processing (and the right to have his or her personal data processed for no other purpose, without his or her consent);
- The right to have access to his or her personal data, including the right to review it and obtain a copy thereof in a clear format and at no charge (subject to any charges permitted in respect of credit information);
- The right to have inaccurate personal data corrected or updated; and
- The right to have personal data destroyed when it is no longer required for the purpose for which it was originally collected.

Data controllers are required to respond to requests by data subjects to exercise their rights in accordance with the time period and means to be specified in the Regulations. There is also a requirement to specify the rights of the data subject in the privacy policy to be communicated to the data subject prior to personal data being collected and processed.

There is a restriction on the use of personal data, such as email addresses and postal addresses, to send promotional materials. This restriction does not apply to awareness-raising materials issued by government entities, or where the contact details are collected directly from the data subject and the consent of the data subject has been obtained in advance, or where there is a clear opt-out mechanism for such communications. (This approach seems broadly consistent with restrictions found in the CITC's anti-SPAM regulations.)

When personal data is collected directly from the data subject, certain information needs to be communicated to the data subject in advance by way of a privacy policy. This includes:

- The legal basis or practical justification for the proposed personal data processing;
- The purpose of the proposed personal data processing (and the fact that personal data will not be processed for other purposes except as permitted pursuant to the Law);
- The identity and address of the data controller;
- The identity of any entities to which the personal data will be disclosed, and in what capacity;
- Whether the Personal Data will be transferred, disclosed, or processed outside Saudi Arabia;
- The implications of not processing personal data in the manner contemplated;
- The data subject rights as contemplated in the Law; and
- Other considerations (to be specified in the Regulations), depending on the nature of the data controller's activity.

With regard to accuracy, the Law requires data controllers to take adequate steps to verify that personal data is accurate, complete, and kept up-to-date. The Law also requires data controllers to ensure that any entity to which personal data has been disclosed is notified of any changes/amendments to such personal data. The Regulations are to specify further details in terms of timelines to which the obligation to update applies, along with procedures for managing the impact of processing inaccurate or outdated personal data.

Governance, security and breach notification

When selecting a data processor, data controllers must choose data processors able to give effect to the provisions of the Law and Regulations. There is an obligation on data controllers to ensure data processors continue to comply with their obligations, in a manner consistent with the Law and Regulations, and without prejudice to the rights of the data subject or the requirements of the competent authority.

Generally, a data controller may only disclose personal data personal data in limited circumstances, including:

- With the consent of the data subject;
- If the personal data is collected from a publicly available source;
- When the entity requesting disclosure is a public entity and the contemplated processing is required for national security or the administration of justice.
- If disclosure of the personal data is necessary for protecting the public health or the life or health of an individual or specific individuals; and
- If the disclosure will be limited to processing in a manner that makes it impossible to identify the data subject.

The Law sets out restrictions on disclosures applicable to some of these scenarios, including where the disclosure poses a risk to national security, affects the integrity of ongoing criminal investigations, violates the privacy of another data subject, or breaches professional or other confidentiality obligations.

There is a requirement to destroy personal data after the purpose for which it was collected has been achieved. If the data is anonymised, this requirement no longer applies; nor does it apply in circumstances where there is a legal justification for retaining it, or where the personal data is closely related to legal proceedings and needs to be kept for such purpose.

Data controllers are required to apply appropriate technical and organisational measures to ensure the security of personal data, in accordance with the provisions of the Regulations. In the event of a data breach incident, whether it be a leak, unauthorised access, or unintended destruction, there is an obligation to notify the competent authority. If such incident could cause serious damage to the personal data or to the data subject, there is also an obligation to notify the data subject.

The concept of ‘privacy impact assessment’ appears in the form of an obligation on the data controller to evaluate the personal data protection implications of any product or service provided by the data controller.

Processing data for scientific, research or statistical purposes is permitted, without the consent of the data subject, if the identity of the data subject is removed or will be destroyed in the course of the processing. (There is a limitation to this latter exception in the context of sensitive personal data, although the rationale behind this is not entirely clear.) Other exceptions apply, and we expect further detail in the Regulations.

The Law contemplates each data controller appointing one or more employees to perform a data protection officer type function, being responsible for compliance with the Law and Regulations. There is no threshold element, and we expect that further detail in this regard will be made available in the Regulations.

Data transfers

In terms of transfers of personal data outside the Kingdom, there is considerable ambiguity. Our reading is that, except to protect the vital interests of the data subject (where a transfer is, presumably, permitted),

the transfer of personal data to a recipient outside the Kingdom is only permitted to fulfil an obligation falling on the Kingdom, or otherwise in the Kingdom's interests, or for other purposes to be specified in the Regulations, if all the following requirements are met:

- The transfer is not prejudicial to national security;
- The recipient shall provide adequate guarantees in respect of protecting the personal data in a manner no less stringent than as provided in the Law and Regulations;
- The personal data being transferred is the minimum necessary for the purposes contemplated; and
- The competent authority shall approve the proposed transfer in accordance with the Regulations.

Except where personal data is sensitive data, and with the exception of the requirement above relating to national security, the competent authority may exempt a data controller from meeting these requirements if it is satisfied that the personal data will enjoy an adequate level of protection in the circumstance. We do not anticipate that that there will be heavy restrictions on transfers of personal data abroad, or that the wording of the transfer-related provision should be read as hinting at a strict data localisation requirement – although it is difficult to say with certainty at this stage.

It will be interesting to see what the Regulations provide, but our reading is that there may still be a requirement to obtain a permit from the competent authority in all instances – and this has potential to be impractical.

Supervision

The competent authority is responsible for supervising the application of the Law and its Regulations. (There is also mention of SAMA and CITC having certain powers – in respect of entities licensed by SAMA and CITC, respectively.) Data controllers are required to comply with the directions of the competent authority, including by providing such documents or information that the authority may require in order to verify compliance with the Law and its Regulations. The competent authority has the power and discretion to delegate aspects of its function to other entities.

There are record keeping obligations on data controllers, and an obligation to make such information available to the competent authority upon demand. At a minimum, the record keeping obligations require data controllers to keep the following:

- Contact details of the data controller;
- Purpose of the processing activities;
- Description of the categories of data subjects;
- Identity of any entity to which personal data will be disclosed;
- Whether any personal data will be transferred to an entity outside Saudi Arabia; and
- Expected personal data retention timeframe.

The Law contemplates the competent authority establishing a dedicated online portal through which data controllers will be required to register the fact of their data processing activities, and pay an associated fee of no more than SAR100,000 (about USD27,000). (We would expect that there will be a sliding scale, as a fee of this magnitude would be onerous for many businesses.) The portal shall also provide record keeping functionality, as per the record keeping obligations mentioned above.

Foreign data controllers located outside Saudi Arabia that process personal data relating to data subjects in the Kingdom will be required to appoint a representative in Saudi Arabia responsible for meeting the requirements set out in the Law and the Regulations. (As noted above, this requirement is not being implemented immediately; there is a long-stop deadline of five years within which the competent authority will be required to implement this requirement.)

Remedies

The Law permits aggrieved data subjects to submit a complaint to the competent authority in respect of any issue arising from the Law and Regulations, and further details on the complaint process are expected in the Regulations. The aggrieved party may also file a claim for damages before the competent court.

Under the Law, the unlawful discourse of sensitive data attracts serious penalties, namely imprisonment for up to two years and/or a fine of up to SAR3,000,000 (about USD 800,000). Failure to comply with the requirements relating to transfers of personal data also attracts significant penalties, namely imprisonment for up to one year and/or a fine of up to SAR1,000,000 (about USD 270,000). These constitute criminal offences, which would be investigated by the Public Prosecutor. Recidivism can attract penalties of up to twice the maximums contemplated in the Law.

The Law also provides for fines of up to SAR5,000,000 (about USD1,350,000) in respect of failure to comply with the requirements of the Law and its Regulations other than those specified above. (Again, recidivism can attract penalties of up to twice the maximums contemplated in the Law.) The competent court can also confiscate funds generated from violations of the law.

The competent authority will appoint officers to identify violations, and may seize equipment as part of its investigation. The competent authority will also establish a violations committee responsible for assessing such violations and determining the appropriate penalties. The decisions of the violations committee may be appealed to the competent court.

A further penalty available in respect of violations that become the subject of a final court decision or a final judgement of the violations committee is publication of the decision in a local newspaper.

The Law also provides for obligations of confidentiality for entities and personnel involved in personal data processing, and penalties for breach of such obligations.

For further information, please contact Nick O'Connell