Grant Thornton

كليد اند كو
CLYDE&CO

Personal Data Protection Law

– the impact to Saudi based businesses

grantthornton.sa

Saudi Arabia has issued its first comprehensive national data protection law to regulate the collection and processing of personal information. The law will accelerate Saudi Arabia's digitization efforts while helping to create an information-based society.

In collaboration with Clyde & Co we explore the details of the legislation, along with sharing insights from Grant Thornton's Advisory Director, on the operational implications.

What is the new law?

The Personal Data Protection Law (PDPL) was implemented by Royal Decree M/19 of 9/2/1443H (16 September 2021) approving Resolution No. 98 dated 7/2/1443H (14 September 2021). It was published in the Official Gazette on 24 September 2021.

The Saudi Data & Artificial Intelligence Authority (SDAIA) will supervise the implementation of the new legislation for the first two years, following which a transfer of supervision to the National Data Management Office (NDMO) will be considered. The NDMO is the regulatory arm of SDAIA and had previously published interim data governance regulations in 2020, which we assume have now been superseded by the PDPL insofar as they relate to personal data protection.

According to SDAIA's announcement, the PDPL is intended to ensure the privacy of personal data, regulate data sharing and prevent the abuse of personal data in line with the goals of the Kingdom's Vision 2030 to develop a digital infrastructure and support innovation to grow a digital economy.

Who and what is within the scope of the PDPL?

The PDPL is designed to protect "personal data", i.e., any information, in whatever form, through which a person may be directly or indirectly identified. This expressly includes an individual's name, identification number, addresses and contact numbers, photographs, and video recordings of the person.

The PDPL applies to any processing by businesses or public entities of personal data performed in Saudi Arabia by any means whatsoever, including the processing of the personal data of Saudi residents by entities located outside the Kingdom. The PDPL does not apply to the processing of personal data for personal and family use.

What are the main features of the PDPL?

Many of the features of the PDPL are consistent with concepts and principles contained in other international data protection laws, for example:

- Data subject rights: Individuals (data subjects) will, subject to some exceptions, have the right to be informed of personal data processing and the legal basis of such processing, the right to access their personal data (including to obtain a free of charge copy of the same), the right to correct or update their personal data, and the right to request its destruction if no longer needed. Data subjects also have the ability to file complaints relating to the application of the PDPL with the regulatory authority.

- Controller registration: Organisations that collect personal data and determine the purpose for which it is used, and the method of processing (controllers) will be required to register on an electronic portal that will form a national record of controllers. There will be an annual fee payable for registration to be determined in executive regulations (which are to be issued in due course).

- Controller obligations: Controllers will be obliged to ensure the accuracy, completeness, and relevancy of personal data before processing it, to maintain a record of processing for a period that will be prescribed by the executive regulations, and to ensure that staff are suitably trained in the PDPL and data protection principles.

- Consent: Data subjects may withdraw their consent to the processing of personal data at any time and consent must not be a pre-requisite for the controller to offer a service or benefit (unless the service or benefit is specifically related to the processing activity for which consent is obtained).

- Non-consent-based processing: Notwithstanding the provisions on withdrawal of consent, the PDPL makes clear that data processing does not always require the consent of the data subject. Consent is not required if the processing

would achieve a clear benefit and it is impossible or impractical to contact the data subject, if it is required by law or prior agreement to which the data subject is a party, or if the controller is a public entity and the processing is required for security or judicial purposes.

- Privacy policy: Controllers are required to implement a privacy policy and make it available to data subjects prior to the collection of their personal data. The PDPL sets out the minimum information that should be included in the privacy policy, including when personal data is collected directly from the data subject.

- Purpose limitation and data minimisation: Organisations are required to make clear the purpose for which personal data is collected and used. Personal data should also be relevant, and controllers should limit collection to the minimum amount required to achieve the intended purpose.

- Impact assessments: Controllers are required to evaluate the impact of processing personal data and, if personal data is no longer needed to achieve the intended purpose, the controller should stop the collection of such data.

- Marketing: Personal data may not be used for marketing purposes without the consent of the recipient or use of opt-out mechanisms.

- Breach notification: Data breaches, leakages or unauthorised access to personal data must be notified to the supervising authority and incidents that cause material harm to the data subject must be notified to data subjects.

How does it differ from other international laws?

While the PDPL contains many aspects that are similar to the GDPR and other data protection laws around the world, there are a number of unique aspects:

- The PDPL operates a more stringent approach to data sovereignty than many comparable laws with controllers not able to transfer personal data outside Saudi Arabia unless required to comply with an agreement to which the Kingdom is a party, to serve Saudi interests or for other purposes that will be set out in the executive regulations. In any case, there are further requirements to ensure that the data transfer or disclosure to a party outside the Kingdom does not impact national security or Saudi interests and to obtain the approval of SDAIA.

- Apart from data transfers, there is also a caveat to the usual permitted disclosures of personal data by the controller if the disclosure could pose a security risk, damage the reputation of the Kingdom or impact Saudi Arabia's relationship with other countries.

- There are several obligations on the controller to destroy personal data in certain circumstances, although the controller may be able to retain de-identified data or personal data that is required to be retained by law or in the context of legal proceedings.

- Unlike other international data protection laws, the PDPL also applies to the data of deceased persons if it can lead to the specific identification of the deceased person or his or her family.

- The breach notification provisions are stricter than many international laws with requirements to notify "immediately" rather than within a specified period. It is possible that the notification process may be further clarified by the executive regulations.

There is a tacit acknowledgement that the PDPL may further evolve with a number of the opening provisions referring to coordination between SDAIA and other relevant entities to review and amend the PDPL both during the first year after the PDPL becomes effective and over a longer five-year timeline. There are also provisions suggesting that further details will be issued in respect of the processing of health and credit data and that SDAIA will liaise with the Kingdom's financial and ICT regulators to align with existing rules in those sectors.

What are the penalties for non-compliance?

The disclosure or publication of sensitive data contrary to the PDPL may result in penalties of imprisonment for up to two years or a fine of up to SAR 3,000,000 (US$ 800,000).

Violation of the data transfer provisions could result in imprisonment for up to one year and a fine of up to SAR 1,000,000 (US$ 266,600).

In respect of all other provisions of the PDPL, the penalties are limited to a warning notice or a fine of up to SAR 5,000,000 (US$ 1,333,000).

Any of the fines could also be increased up to double the stated maximums for repeat offences and the court may order confiscation of funds gained as a result of breaching the law and/or require publication of the judgment in a newspaper or other media at the offender's expense.

Parties affected by the offences may be able to claim compensation.

The operational impact.

The rapidly changing privacy landscape is driving smarter privacy practices. Businesses will now need to consider the impact which the PDPL will have on operations.

Leaders will need to consider the five core aspects of their enterprise model, which include:

- Gap Analysis

Review and identify the core operational processes within the organisation, identifying the key touchpoints which either require or hold personal data. A thorough gap analysis should be conducted to enable processes to be rectified accordingly.

- Compliance Audit

Assess compliance with the requirements of the PDPL following a holistic risk-based approach, to ensure key compliance risks are appropriately mitigated through robust controls.

- Governance

Business leaders will need to ensure thorough policies, procedures, and frameworks have been developed to enforce compliance with the requirements.

- Training & Development

Skill development and raising awareness amongst employees and operational teams is essential to enable compliance with the PDPL and regulations.

- Compliance Programme

Leaders will need to consider building and translating a comprehensive compliance program covering the requirements across the organization. Likewise, this programme should make privacy an essential part of the enterprise value chain, with business leaders ensuring they continuously monitor their data privacy risks and enhance their competitive advantage in the marketplace.

What happens next?

The PDPL is stated to take effect 180 days after its publication in the Official Gazette, which means that it will be effective from 23 March 2022. The executive regulations supplementing the Law should also be issued within this period.

However, the implementing decree provides that:

- The requirement for entities located outside the Kingdom that process the personal data of Saudi residents to appoint a representative in the Kingdom and comply with the PDPL shall be delayed for a period of up to five years from the effective date (to be determined by SDAIA).

- Controllers will be required to adjust their status in accordance with provisions of the PDPL within a period not exceeding one year from the date that it becomes effective (and that period may be further extended for certain entities).

Accordingly, it seems that there will be a transitional period of at least 18 months until the PDPL is fully enforceable against local entities (and potentially longer for organisations based outside the Kingdom). The Council of Ministers' approval in the Resolution also notes that SDAIA will coordinate with the Saudi Central Bank and Communications and Information Technology Commission (CITC) to address the application of the PDPL to regulated financial institutions and ICT service providers respectively.

We anticipate that further details and guidance will be published during the period prior to the PDPL taking effect on matters such as the mechanisms and procedures for obtaining regulatory consent or notifying breaches. The timescales for implementation may also be clarified by further announcements and there is provision in the PDPL for SDAIA to review and suggest amendments within the first year from the effective date.

In any case, all businesses operating in Saudi Arabia or processing the data of Saudi residents will now need to start assessing their activities and making changes to align with the PDPL. Controllers will be required to hold training for staff on the terms and principles of the PDPL and will need time to ensure that a culture of data protection is suitably embedded into the organisation.

To discuss the legislation and its operational impact to your business, contact the technical specialists:

Dino Wilkinson
Partner
Clyde & Co

T +971 2 494 3595
E dino.wilkinson@clydeco.com

Ahmad Al Zoubi
Director
Grant Thornton, KSA

M +966 59 5370053
E aalzoubi@sa.gt.com

Masha Ooijevaar
Associate
Clyde & Co

T +971 4 384 4117
E masha.ooijevaar@clydeco.com

Waqas Ahmed
Manager
Grant Thornton, KSA

M +966 50 8292913
E waqas.ahmed@sa.gt.com

Head office

Riyadh
Al Mousa Commercial Complex,
7th Floor, Tower 4,
Al Olaya Street,

T +966 (11) 463 0680
E infor@sa.gt.com

Khobar

Ababtain Tower,
7th Floor,
Dhahran Street

T +966 92 000 6582
E infok@sa.gt.com

Jeddah

Saad H. Abu Khadra Building,
3rd Floor, King Fahad Street,
P.O. Box 20142,

T +966 (11) 463 0680
E infoj@sa.gt.com

Aldar Audit Bureau
Abdullah Al-Basri & Co.
Member firm of Grant Thornton International Ltd.
Grant Thornton

grantthornton.sa