DATA PROTECTION LAWS OF THE WORLD

Saudi Arabia

DLA PIPER

Downloaded: 21 May 2024

SAUDI ARABIA

Last modified 23 February 2024

LAW

The Personal Data Protection Law (issued pursuant to Royal Decree No. M/19 of 9/2/1443 H (corresponding to 16 September 2021), as amended by Royal Decree No. M/148 dated 5/9/1444H (corresponding to 27 March 2023)) ("**PDPL**") came into effect on 14 September 2023, but data controllers have a further year in which to comply (although that period may be further extended for certain entities). Accordingly, businesses within the scope of the PDPL will have until 14 September 2024 to adjust their status to become compliant with the PDPL.

The Implementing Regulations are also now in force, and provide further detail and guidance on various requirements in the PDPL. It comprises of two connected regulations, with the first being the 'Implementing Regulations to the PDPL', and the second being the 'Regulations on Personal Data Transfers outside the Kingdom' ("**Transfer Regulations**").

The PDPL is a law that applies on a national level and will apply to all sectors, with certain limited exceptions. For this reason, the PDPL will need to be considered in the broader legal and regulatory framework of the Kingdom of Saudi Arabia ("**KSA**"), with other sector specific frameworks such as those issued by the Saudi Central Bank, National Cybersecurity Authority or Communication, Space and Technology Commission ("**CST**").

DEFINITIONS

Definition of personal data

Personal data is defined as "*every data – of whatever source or form – that would lead to the identification of the individual specifically, or make it possible to identify him directly or indirectly, including: name, personal identification number, addresses, contact numbers, license numbers, records, personal property, bank account and credit card numbers, fixed or moving pictures of the individual, and other data of personal nature.*"

Definition of sensitive personal data

Sensitive data is defined as "*every personal data that includes a reference to an individual's ethnic or tribal origin, or religious, intellectual or political belief, or indicates his membership in nongovernmental associations or institutions, as well as criminal and security data, biometric data, genetic data, credit data, health data, location data, and data that indicates that both parents of an individual or one of them is unknown.*"

NATIONAL DATA PROTECTION AUTHORITY

The Saudi Authority for Data and Artificial Intelligence ("**SDAIA**") will be the data regulator for at least two years. During this time, consideration will be given to transferring the competence to supervise the application of the PDPL (and its Implementing Regulations) to the National Data Management Office.

The Saudi Central Bank and the CST both appear to maintain their jurisdiction to regulate data protection within their remit.

REGISTRATION

The PDPL has introduced a potential requirement for data controllers to register with SDAIA. It is expected that SDAIA will issue rules regarding such registration and will specify which data controllers must register.

DATA PROTECTION OFFICERS

The PDPL clarifies when a data controller must appoint a data protection officer. This includes where the data controller is a public entity that provides services involving the processing of personal data on a large scale, where the primary activities of the data controller consist of processing operations that require regular and continuous monitoring of individual also on a large scale, and where the core activities of the data controller consist of processing sensitive data.

COLLECTION & PROCESSING

The PDPL applies to any processing of personal data related to individuals that takes place in KSA by any means, including the processing of personal data related to individuals residing in KSA by any means by any entity outside KSA.

Under the PDPL, the primary legal basis for processing of personal data is consent of the data subject. However, the PDPL also provides for circumstances where consent is not required for processing of personal data.

TRANSFER

There are detailed rules relating to the transfer of personal data outside of KSA. The PDPL allows for the transfer of personal data outside of KSA for several purposes (for example, if such action is taken to meet an obligation to which the data subject is a party) and subject to various conditions (for example, the transfer or disclosure must not compromise the national security or vital interests of KSA and be limited to the minimum amount of personal data needed).

Subject to such requirements and conditions, the Transfer Regulations have introduced a number of circumstances where a cross border transfer of personal data is permissible. This includes to countries with appropriate levels of protection and no less than the protections afforded under the PDPL.

However, transfers of personal data to countries which are not deemed as having an adequate level of protection may still be made where "appropriate safeguards" are put in place. If the data controller is unable to use any of the appropriate safeguards, there are still limited cases where cross border transfers are permissible. Such transfers are still however subject to various controls.

In addition, in certain contexts or sectors, specific approvals may be required - for example, in a banking context, approval from the Saudi Central Bank.

SECURITY

Data controllers must take necessary organisational, administrative and technical measures and means to ensure personal data is preserved, including when it is transferred, in accordance with the provisions and controls specified in the Implementing Regulations.

BREACH NOTIFICATION

The PDPL imposes data breach notification requirements on data controllers, to notify the regulator (i.e. SDAIA) and / or impacted data subjects, depending on the circumstances. Where a notification is required to SDAIA, the data controller must notify within 72 hours of becoming aware of the breach. Where a notification is required to impacted data subjects, this must be made without undue delay.

In addition, notification obligations may be triggered in specific contexts / sectors – for example, cloud service providers may be required to report security breaches to the CST depending upon the circumstances.

ENFORCEMENT

Under the PDPL, the following penalties apply with respect to violations:

- Disclosure or publication of sensitive data in violation of the PDPL with intent to harm the data subject or to achieve a personal benefit, is punishable by imprisonment for up to two years and/or a fine up to SAR 3 million;
- For other breaches of the PDPL not covered by the previous point, this is punishable by a warning or by a fine not exceeding SAR 5 million. Separately, SDAIA has the power to issue warnings / administrative fines of up to SAR 5 million for any other violation, which is appealable. This is without prejudice to any more severe penalty stipulated in another law.

Note, the competent court may double the penalty of a fine for repeat offenders (even if this results in exceeding the maximum limit(s) set out above, provided that it does not exceed double the limit(s)).

Further, the competent courts may order confiscation of funds obtained as a result of committing violations (without prejudice to bona fide third party rights). The competent courts / committee may also order publication of a summary of the judgement or decision at the violator's expense.

Any person who suffers harm as a result of violation of the PDPL has a right to claim compensation before the competent court for material or moral damage.

ELECTRONIC MARKETING

There are specific rules in KSA relating to the use of personal data for marketing purposes. The PDPL and its Implementing Regulations contain various conditions around when personal data may be processed for the purposes of direct marketing. Additional requirements may also apply in certain contexts – for example, in the context of e-commerce activity.

ONLINE PRIVACY

There is no specific legislation in the KSA that specifically regulates the use of cookies.

KEY CONTACTS

Mohamed Moussallati
Legal Director
T +966 11 288 5449
mohamed.moussallati@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.