DATA PROTECTION LAWS OF THE WORLD

Saudi Arabia

DLA PIPER

SAUDI ARABIA

Last modified 19 January 2023

LAW

The data protection landscape in the Kingdom of Saudi Arabia ("**KSA**") is primarily (but not exclusively) regulated by the following:

- Personal Data Protection Law ("**PDPL**") when it comes into effect; and
- Personal Data Protection Interim Regulations ("**PDPIR**") issued by the National Data Management Office ("**NDMO**").

The PDPL was published in the KSA Official Gazette on 24 September 2021 and was intended to come into effect by 23 March 2022. However, the Saudi Data and Artificial Intelligence Authority ("**SDAIA**") announced that the full enforcement of the PDPL would be postponed until 17 March 2023 in order for "necessary changes" to be made, and this was confirmed by the issuance of Royal Order No. 51627 which provides that the implementation of the PDPL will be postponed for a period of 540 days from the date of its publication in the KSA Official Gazette (published on 24 September 2021). It is therefore expected that the published version of the PDPL will be superseded by an amended version of the law.

Indeed, long expected proposed amendments to the published version of the PDPL were released for public consultation on 20 November 2022 and expired on 20 December 2022. We have provided comments in this Handbook against the originally published version of the PDPL and not the version that underwent public consultation. However, it is important to note that the PDPL (and the proposed amendments released for public consultation) may be subject to change once the final form of the PDPL is approved / issued, and that the PDPL is not currently effective.

In the meantime, while the PDPL is not effective as law, the PDPIR is, as we understand it, in effect now.

Both the PDPIR and the PDPL have extra-territorial effect. In particular (subject to limited exceptions):

- The PDPIR applies to all entities in KSA that process Personal Data in whole or in part, as well as entities outside of KSA that process Personal Data related to individuals residing in KSA using any means, including online Personal Data 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 of KSA.

There may also be specific regulations applicable to certain industries / sectors, for example, in banking, which is regulated by the Saudi Central Bank (previously known as the Saudi Arabian Monetary Authority).

DEFINITIONS

Definition of personal data

Under the PDPIR, Personal Data is defined as *"Any element of data, regardless of source or form whatsoever, which independently or when combined with other available information could lead to the identification of a person including but not limited to: first name and last*

name, Saudi national ID number, addresses, phone, number, bank account number, credit card number, health data, images or videos of that person."

Under the PDPL, 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

Under the PDPIR, Sensitive Data is defined as "*Data, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of government programs, or the privacy to which individuals are entitled.*"

Under the PDPL, 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

As per the PDPL, the 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 Executive Regulations) to the NDMO.

The Saudi Central Bank and the Communications, Space and Technology Commission ("**CST**") both appear to maintain their jurisdiction to regulate data protection within their remit.

REGISTRATION

The PDPIR does not impose registration requirements.

As per the PDPL, Data Controllers must register with SDAIA. There will be a fixed fee for private entities that are Data Controllers, which is yet to be published in the Executive Regulations of the PDPL.

In addition, under the PDPL, records of processing activities ("**ROPA**") need to be registered with SDAIA. Like other data protection laws, the PDPL appears to require that the Data Controller prepares a ROPA. However, unlike other data protection laws, the PDPL indicates that the ROPA must also recorded with SDAIA.

DATA PROTECTION OFFICERS

There is no specific requirement under the PDPIR for organisations to appoint a data protection officer.

As per the PDPL, foreign Data Controllers must appoint a representative in KSA to be licensed by the "competent authority" (as per the PDPL, this is to be determined by a decision of the Cabinet) to perform the Data Controller's obligations stipulated under the provisions of the PDPL and the Executive Regulations (once issued).

This appointment does not prejudice the responsibilities of this foreign Data Controller towards the Data Subject or SDAIA. The Executive Regulations are to set out the provisions related to licensing and the limits of the representative's relationship with the Data Controller outside KSA, which he represents.

COLLECTION & PROCESSING

As per the PDPIR, Personal Data may not be collected or processed without the Data Subject's express consent. "Consent" is defined as "*a knowing, voluntary, clear, and specific, expression of consent, whether oral or written, from the Data Subject signifying agreement to the processing of personal data.*"

As per the PDPL, the primary basis for processing is consent of the Data Subject. The Executive Regulations will outline the "*cases*

in which the consent must be in writing". This indicates that there may be cases in which consent can be collected by means other than in writing. However the PDPL itself does not refer to a concept of processing for "legitimate interests" in the same manner as the GDPR, and indeed as other data protection frameworks in the region allow for.

Rather, the PDPL allows for processing other than on the basis of consent if:

- the processing achieves a "definite interest" (not defined) of the Data Subject and it is impossible or difficult to contact the Data Subject;
- if the processing is in accordance with another law, or in the implementation of an earlier agreement to which the Data Subject is a party; and
- if the Data Controller is a public entity and such processing is required for security purposes or to meet judicial requirements.

TRANSFER

Under the PDPIR, Data Controllers may only store and process Personal Data outside KSA after obtaining written approval from the relevant "Regulatory Authority" and the Regulatory Authority must coordinate with the NDMO.

"Regulatory Authority" is defined as "*Any independent governmental or public entity assuming regulatory duties and responsibilities for a specific sector in KSA under a legal instrument.*"

In the event Data Controllers are not subject to specific Regulatory Authorities, then the NDMO will exercise the roles and functions of such authorities.

Data Controllers must also obtain NDMO's approval, having coordinated with the Regulatory Authority, prior to sharing Personal Data with other entities outside of KSA.

Under the PDPL, data transfers out of KSA are even more tightly controlled than under the PDPIR. Personal Data transfers outside of KSA are prohibited except in the following circumstances:

- extreme necessity to preserve the life of a Data Subject outside of KSA or the Data Subject's "vital interests";
- to prevent, examine or treat a disease;
- if the transfer is in implementation of an obligation under which the KSA is a party;
- to serve the interests of KSA; or
- other purposes as determined by the Executive Regulations (yet to be issued).

However, the above is still predicated upon complying with the following conditions:

- the transfer or disclosure does not prejudice national security or the vital interests of KSA;
- there are sufficient guarantees for preserving the confidentiality of the Personal Data to be transferred or disclosed, so that the standards are not less than the standards in the PDPL and the Executive Regulations;
- the transfer or disclosure must be limited to the minimum Personal Data needed; and
- the competent authority approves the transfer or disclosure, as determined by the Executive Regulations.

However, the competent authority may exempt the Data Controller, on a case-by-case basis, from being bound by these conditions if:

- the transfer does not prejudice national security or the vital interests of KSA;
- if the competent authority, jointly or severally with other parties, sees that the Personal Data will have an acceptable level of protection outside of KSA; and
- the Personal Data is not Sensitive Data.

Note also that the relevant definitions for "processing" under both the PDPIR and PDPL include, amongst other things, transfer of Personal Data, and so the consent requirements relating to processing are also relevant / applicable.

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

The PDPIR and PDPL are not prescriptive about specific technical standards or measures with regards to specific security requirements.

However, the PDPIR does provide that Personal Data should be protected from leakage, damage, loss, theft, misuse, modification, or unauthorised access according to the controls issued by the National Cybersecurity Authority and other relevant authorities.

Similarly, the PDPL provides that the Data Controller must take the 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 Executive Regulations.

BREACH NOTIFICATION

Under the PDPIR, Data Controllers must notify the Regulatory Authorities immediately, and no later than 72 hours, in the event of any data breach or leakage impacting Personal Data in accordance with the mechanisms and procedures determined by the Regulatory Authorities. In the event Data Controllers are not subject to specific Regulatory Authorities, then the NDMO will exercise the roles and functions of such authorities.

Under the PDPL, Data Controllers must notify the competent authority (as per the PDPL, this is to be determined by a decision of the Cabinet) as soon as it becomes aware of the occurrence of a leakage or damage of Personal Data, including if Personal Data was illegally accessed. In addition, the Executive Regulations will specify circumstances in which the Data Controller must notify the Data Subject in the event of a leakage or damage of the Data Subject's Personal Data or illegal access thereto. However, if the occurrence of any of the above would cause serious harm to the Data Subject's data or the Data Subject, the Data Controller must notify the Data Subject immediately.

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

The PDPIR does not contain any express enforcement mechanism or penalties for non-compliance.

As per the PDPL, there are criminal penalties and fines for the following offences:

- unlawfully transferring data out of KSA (imprisonment of up to 1 year and / or a fine of up to SAR 1 million); and
- disclosing or publishing Sensitive Data unlawfully with intent of harming the Data Subject or with the intention of achieving some personal benefit (imprisonment up to 2 years and / or a fine of up to SAR 3 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.

ELECTRONIC MARKETING

There are specific rules around the use of Personal Data for marketing purposes in the PDPL. This includes that Data Controllers must not use personal means of communications, including postal and electronic addresses, of the Data Subject in order to send promotional or awareness materials without first obtaining the consent of the Data Subject, and providing the Data Subject with a mechanism to opt-out.

Additional requirements may also apply in specific 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.

Assuming the relevant cookies will collect, process or transfer Personal Data, then, under the PDPIR and, once in effect, the PDPL, it is generally recommended that opt-in consent is secured in relation to 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.