Baker McKenzie.

Client Alert

May 2024

Saudi Arabia: Next steps for compliance with Personal Data Protection Law as one-Hijri-year grace period expiry approaches

In brief

As you may know, on 14 September 2023, the Personal Data Protection Law (PDPL) promulgated by Royal Decree No. M/19, dated 09/02/1443H, amended pursuant to Royal Decree No. M/148, dated 05/09/1444H, officially entered into force in the Kingdom of Saudi Arabia.

While the PDPL came into force on 14 September 2023, organizations were afforded a further 12 Hijri months' period from the date of entry into force to bring themselves into compliance with the PDPL (i.e., on or around 2 September 2024). There should have been no enforcement action during the intervening period. We have prepared a timeline of events relating to the PDPL in this article.

In this issue

There will be different timelines for enforcement that will be applied to certain sector-specific entities (e.g., financial institutions, private entities working primarily with government and public organizations, etc.) and that will be communicated by the relevant authority for each sector. In certain situations, these will be shorter than the general timeline for enforcement (i.e., prior to the 14 September 2024). This will require businesses and organizations to remain vigilant in their efforts to ensure compliance with the PDPL to safeguard the privacy and security of individual's personal information.

Timeline of events leading to the PDPL's entry into force

Date (Gregorian)	Event	Effect
16 September 2021G	The PDPL is promulgated by Royal Decree No. M/19 dated 09/02/1443H.	The PDPL stated that it shall enforce 180 days after its publication in the Official Gazette.
24 September 2021G	The PDPL is published in Official Gazette.	The effective date of the PDPL was originally set for 23 March 2022G.
11 March 2022G	Royal Order No. 51627 dated 18/08/1443H is issued.	The effective date of the PDPL was postponed 540 days after its original publication in the Official Gazette, falling on 17 March 2023G.
27 March 2023G	Royal Decree No. M/148 dated 05/09/1444H amending the PDPL is issued.	The amended PDPL states that it shall enter into force 720 days after its original publication in the Official Gazette, falling on 14 September 2023G.

7 September 2023G	Implementing Regulations and Data Transfer regulations are officially published.	The Implementing Regulations and the Data Transfer Regulations under the PDPL are officially published in their definitive version (following a public consultation closed on 31 July 2023G).
14 September 2023G	The PDPL officially entered into force—start of the one-Hijri-year grace period.	The PDPL enters into force in the Kingdom of Saudi Arabia. Controllers will still have a one-Hijri-year grace period from the date of entry into force (ending on 2 September 2024G), to comply with its requirements, including its Implementing Regulations and Data Transfer Regulations.
2 September 2024G	End of the grace period—start of the enforcement by the Competent Authority.	The grace period afforded to organizations for organizing their compliance with the PDPL will end. The Competent Authority will start to undertake enforcement action against organizations that are breaching the provisions of the PDPL.

In more detail

What is the PDPL?

Before the introduction of the PDPL, there was no standalone data protection law in Saudi Arabia that addressed the regulation of privacy across the board. Only certain rights existed in the form of Shari'ah principles and certain discrete provisions in laws, regulations, and other legal sources that regulate data protection in connection with the use of specific technologies or in respect of certain types of entities or services. The entry into force of the PDPL was a significant development in Saudi Arabia's legislative landscape that will have implications for almost all entities operating in Saudi or who offer their services to Saudi customers.

The PDPL was developed by the Saudi Data and Artificial Intelligence Authority (SDAIA), which will act as the competent governmental authority to administer the PDPL ("**Competent Authority**") for a period of two years, but it may thereafter transfer such competence to the National Data Management Office (NDMO). The publication of the PDPL was completed by the release of the general Implementing Regulations of the PDPL issued on 22/02/1445H (7 September 2023G) ("**Implementing Regulations**") and the Regulations on the Transfer of Personal Data Outside the Kingdom issued on 22/2/1445H (7 September 2023G) ("**Data Transfer Regulations**"). Both the Implementing Regulations and the Data Transfer Regulations provide indispensable details on the compliance obligations arising from the PDPL.

The overarching purpose of the PDPL is to ensure that the processing of all information (or data) relating to an individual ("**Data Subject**"), regardless of its form, that would allow such Data Subject to be identified, whether directly or indirectly ("**Personal Data**"), satisfies certain mandatory requirements to ensure the Data Subject's rights of privacy are protected. For the purposes of the PDPL, "processing" is defined broadly as any action conducted on Personal Data, including, amongst other actions, collection, storage, modification, dissemination, and transmission.

The PDPL aims to regulate (i) the processing of Personal Data that takes place in Saudi Arabia and (ii) the processing of Personal Data of a Saudi resident that takes place outside of Saudi Arabia (i.e., by a controller situated outside of the Kingdom).

In summary, the PDPL can be split into the following key aspects:

- It grants mandatory rights to Data Subjects over their Personal Data.
- It establishes the default position that processing of Personal Data is subject to the Data Subjects' consent unless another legitimate legal basis is satisfied.
- Subject to limited exceptions, it imposes obligations on all Controllers (natural and corporate; public and private) that process Personal Data.

What's next for Controllers?

The PDPL imposes several new obligations on Controllers and we have included below an overview of a number of these obligations:

- **Fair processing notification**: Controllers must inform Data Subjects amongst others of the following:

  i) Legal or practical justification for the collection.
  ii) Purpose of collection, and whether the collection of certain types of Personal Data is required to meet such purpose (i.e., is the processing necessary).
  iii) Controller's identity and address.
  iv) Entity or entities to which the Personal Data will be disclosed, their capacity, including whether it will be transferred, disclosed, or processed outside of Saudi Arabia.
  v) Possible effects and risks of failure to complete the collection of Personal Data (if any).
  vi) Rights of the Data Subject (as provided by the PDPL).

  Controllers must also provide assurances that the Personal Data will not be subsequently processed in a manner inconsistent with the collection purpose unless permitted by the PDPL. We note that much of this information would customarily be included in a privacy policy, the presentation of which is identified as a separate requirement under the PDPL.

- **Privacy policy**: Controllers must adopt and present a privacy policy to Data Subjects for review prior to collecting their Personal Data. The privacy policy must, at a minimum, specify the following:

  i) Purpose of the collection.
  ii) Nature of the Personal Data to be collected.
  iii) Collection and storage method and means of processing.
  iv) Manner by which the Personal Data will be destroyed.
  v) Rights of Data Subjects and details of how such rights can be exercised.

- **Data security**: Controllers must implement all necessary organizational, administrative, and technical measures and means to ensure that Personal Data is protected, including during transfers outside of the Kingdom.

- **Data privacy impact assessments**: Controllers must conduct an evaluation of the effects associated with the processing of Personal data in accordance with the requirements of the Implementing Regulations.

- **Data breach reporting**: Controllers must notify the Competent Authority as soon as they become aware that Personal Data has been leaked, damaged, or illegally accessed. The Implementing Regulations specify the instances when the Data Subject must also be informed of a data breach affecting their Personal Data.

- **Data Protection Officer (DPO)**: Controllers must appoint or assign a DPO who will be responsible for achieving compliance with the PDPL.

- **Destruction of Personal Data**: Controllers must destroy Personal Data as soon as the underlying purpose for collection ceases to exist, but such data may be retained if it is anonymized in accordance with the conditions set out in the Implementing Regulations.

- **Record of processing**: Without prejudice to the requirements relating to the destruction of Personal Data, Controllers must maintain a record of processing activities for a period specified by the Implementing Regulations to be made available to the Competent Authority upon request, and must include, amongst others, the following:

  i) Purpose of the processing.
  ii) Entities to which the Personal Data was or will be disclosed.
  iii) Whether the Personal Data was or will be transferred outside of Saudi Arabia.
  iv) Expected retention period.

- **Employee seminars**: Controllers will be required to hold seminars for their employees to familiarise them with the principles of the PDPL.

- **Cross-border transfers of Personal Data:** The PDPL imposes additional requirements on Controllers for transferring Personal Data outside of Saudi Arabia or disclosing Personal Data to an entity outside of Saudi Arabia. These requirements, which are included under the PDPL, have been expanded further within the Data Transfer Regulations.

Penalties

The penalties under the PDPL can be split into two categories, namely specific and general.

- **Specific:** Imprisonment for a period of up to two years and/or a fine up to a maximum of SAR 3,000,000 (equivalent to approx. USD 790,000) for anyone who discloses or publishes Sensitive Personal Data with the intent to harm a Data Subject (repeat breaches may result in the applicable fine being doubled); and

- **General:** The PDPL provides that the Competent Authority will establish a committee to consider alleged breaches and administer fines, which shall consider the violations and impose a warning or fine (up to SAR 5,000,000, equivalent to approx. USD 1,300,000), according to the type, gravity and impact of the violation committed (repeat breaches may result in the applicable fine being doubled).

However, we note that in addition to financial penalties, breaches of the PDPL may give rise to the following penalties:

i) Criminal sanctions.
ii) Confiscation of funds earned in connection with any breach of the PDPL.
iii) Publication of decisions in local newspapers or by any other proper means to highlight the failings of a particular company.

Accordingly, whilst the financial penalties regime under the PDPL is limited as per the above, the confiscation of funds attained in connection with breaches of the PDPL may amount to an arbitrary sum, which will be incredibly difficult to calculate and may give rise to considerable financial amounts imposed on breaching organizations.

We continue to closely monitor developments related to the PDPL in the Kingdom. Should you have any inquiries regarding the implementation of the requirements under the PDPL, feel free to contact one of the Baker McKenzie teams above.

Contact Us

Zahi Younes
Partner
zahi.younes
@bakermckenzie.com

Lucrezia Lorenzini
Associate
lucrezia.lorenzini
@bakermckenzie.com

Maher Ghalloussi
Associate
maher.ghalloussi
@bakermckenzie.com