Highlights of the Personal Data Protection Law

October 28, 2021

Khalid A. AlArfaj
Managing Partner
Khalid@ArfajLaw.com

Faris S. AlYousef
Trainee Associate
Faris.AlYousef@ArfajLaw.com

The Kingdom of Saudi Arabia (the "Kingdom") has issued its first data protection law: the Personal Data Protection Law (the "PDPL"), to regulate the collection and processing of personal data.

The PDPL is issued by Royal Decree (M/19) of 09/02/1443AH (September 16, 2021) it was published in the Official Gazette on 17/02/1443AH (September 24, 2021) providing that the PDPL shall come into force after 180 days from the date of its publication, on 20/08/1443AH (March 23, 2022). Executive regulations are expected to be issued by the enforcement date.

The PDPL was developed by the Saudi Data and Artificial Intelligence Authority (SDAIA), which will be the competent authority (the "Competent Authority") to administer the PDPL for a period of two years, and it may after that transfer the administration of the PDPL to the National Data Management Office (NDMO).

What is the purpose of the PDPL and what is the scoop of its application?

The PDPL comes in line with the technological development in the Kingdom and it emphasizes the importance of protecting the personal data of individuals. The PDPL applies to any personal data processing carried out by a controller, which is any entity that determines the purpose of processing personal data and how it is processed (the "Controller"), whether the data processing is initiated by it or through any entity that processes data on its behalf (the "Processer").

The PDPL applies to any processing that takes place in the Kingdom, including the processing by entities outside the Kingdom of personal data related to individuals residing in the Kingdom. Foreign data Controllers must appoint a licensed representative within the Kingdom to perform the Controller obligations under the PDPL. The PDPL also applies to personal data of a deceased if it would lead to identifying the deceased or one of his or her family members.

The PDPL grants Controllers a period of one year from its enforcement date to comply with it and grants the Competent Authority the right to grant Controllers longer periods to comply. It also grants the Competent Authority the right to review and suggest amendments within the first year and over a five-year period regarding the implementation of some provisions of the PDPL.

What is the difference between Personal Data and Sensitive Data?

The PDPL defines the "Personal Data" as any data that would lead to the identification of the individual specifically or make it possible to identify him or her directly or indirectly. The "Sensitive Data" is defined as any Personal Data that includes a reference to:

- an individual's ethnic or tribal origin.
- an individual's religious, intellectual or political belief.
- information that indicates an individual's membership of civil associations or institutions.
- forensic and security data, biometric data, genetic data, credit data, health data or location data.
- data that indicates that an individual's one or both parents to be unknown.

What rights do the PDPL gives to the Personal Data owner?

The PDPL grants several rights that guarantee the protection of Personal Data, including the following rights:

- The right to be informed. This includes informing the data owner of the legal or practical reasons for collecting his or her Personal Data and the purpose of such collection, and

that his or her data is going to be processed only for the purpose for which he or she was informed of.

- The right to have access to his or her Personal Data with the Controller. This right includes the right to view the Personal Data and to obtain a copy of it without any fees. The Controller may set specific periods for exercising access to the data.
- The right to correct, complete or update his or her Personal Data held by the Controller.
- The right to delete the Personal Data whenever the need for it is over.
- The right to not process the Personal Data nor change the purpose of its processing without the consent of its owner. The owner of the Personal Data may withdraw this consent at any time.

Can data processing be performed without consent?

The PDPL allows the Controller to process data without obtaining a consent only in the following situations:

- If the data processing is in the interest of the data owner, and it is impossible to contact him or her.
- If the processing is in accordance with another law or in implementation of a previous agreement with the data owner.
- If the Controller is a public entity and such processing is required for security purposes or to satisfy judicial requirements.

What are the Controller's obligations?

The PDPL sets obligations on the Controller, including:

1. The Controller must adopt a data privacy policy, and the policy should be available to individuals to view before collecting their data.
2. When choosing a Processor, the Controller must choose an entity that provides the necessary guarantees for the implementation of the PDPL and its regulations, and it must also continuously verify that the Processor has fulfilled its obligations.
3. If the Controller is collecting data directly from the data owner, it must inform him or her of: a) the legal or practical reasons for collecting his or her Personal Data, b) the purpose of collecting such data, c) the information of those who collect it, d) the parties to whom the data will be disclosed to, and e) whether the data will be transferred, disclosed, or processed outside the Kingdom.

4. The Controller may not process Personal Data without taking necessary steps to verify its accuracy, completeness, currentness and relevance to the purpose for which it was collected.
5. The Controller must destroy the Personal Data when the purpose of its collection ceases to exist. The Controller:
    a. May keep the Personal Data, if it removes all information that may lead to identifying its owner.
    b. Must keep the Personal Data until the reason for the keeping is over:
        i. if there is a legal reason to keep it for a specific period, or
        ii. if the Personal Data is related to a case before a judicial authority.
6. The Controller may not transfer Personal Data outside the Kingdom or disclose it to a party outside the Kingdom unless it is in implementation of an obligation under a convention to which the Kingdom is a party, or to serve the interests of the Kingdom, or for other purposes as determined by the regulations, after the following conditions are met:
    a. Sufficient guarantees are provided for preserving the confidentiality of the Personal Data transferred or disclosed.
    b. The transfer or disclosure does not prejudice the national security or the vital interests of the Kingdom.
    c. The transfer or disclosure must be limited to the minimum Personal Data needed.
    d. The Competent Authority must approve the transfer or disclosure.

When is disclosure allowed?

The PDPL Limits the situations in which a Controller is allowed to disclose data to the following:

- If the owner of the Personal Data agrees to the disclosure.
- If the Personal Data was collected by a publicly available source.
- If the disclosure is limited to processing it in a way that does not lead to the identification of the owner or any other individual.
- If the entity requesting disclosure is a public entity and it is for security purposes.
- If the disclosure is to implement another law or fulfill a judicial requirement.
- If the disclosure is necessary to protect health or public safety, or to protect an individual or certain individuals or their health.

The PDPL, however, prohibits disclosure in the first three cases in some situations such as when the disclosure constitutes a security risk, prevents the discovery of a crime, violates another

individual privacy, leads to disclosure of a confidential source, or other situations as stated in the PDPL and regulations. The PDPL also prohibits disclosure when the disclosure conflicts with the interests of the Kingdom, damages its reputation or impacts its relationship with other countries.

What are the penalties for violating the provisions of the PDPL?

- **Criminal Penalties**:
    1. Unlawful disclosure or publishing of Sensitive Data in violation of the provisions of the PDPL with the intent of harming the data owner or achieving personal interest shall be punished with imprisonment of up to two years and/or a fine of up to three million Saudi Riyals (USD $800,000).
    2. Unlawful transfer of Personal Data outside the Kingdom or disclosure to a party outside the Kingdom without the disclosure being in implementation of a convention to which the Kingdom is a party, or if the reason for the transfer is to serve the interests of the Kingdom, or if the aforementioned conditions are not met, shall be punished with imprisonment of up to one year and/or a fine of up to one million Saudi Riyals (USD $266,666.67).
- **Administrative Fines**: The Competent Authority may punish violators of the PDPL with a fine of up to five million Saudi Riyals (USD $1,333,333.33).
- **Court Confiscation Orders**: The courts have the right to confiscate the funds obtained as a result of violating the PDPL.
- **Compensation:** Individuals may seek compensation for damages incurred as a result of violations of the PDPL and its regulations.

Conclusion

Like other international data protection laws, the PDPL is intended to ensure the privacy of Personal Data, prevent its misuse and regulate its sharing. The PDPL will come into force on March 23, 2022. The executive regulations to be issued is expected to clarify the PDPL. Subject to some exceptions, local and foreign data Controllers, to whom the PDPL is applicable, will have one year from the effective date to comply. Controllers shall start taking steps to ensure their compliance with the PDPL.

If you have any questions about the content of this article, please contact us on: info@ArfajLaw.com or visit our website: www.ArfajLaw.com.