Legal Advisors.
Abdulaziz Alajlan & Partners
in association with Baker & McKenzie Limited

Client alert
Alert | September 2021

Personal Data Protection Law Enacted in Saudi Arabia

On 24 September 2021, the long anticipated Personal Data Protection Law, promulgated by Royal Decree No. M/19, dated 09/02/1443H (corresponding to 16 September 2021) ("**Law**"), was published in the Saudi Official Gazette (*Umm AlQura*). The Law was developed by the Saudi Data and Artificial Intelligence Authority (SDAIA), which will be the competent governmental authority ("**Data Authority**") to administer the Law for a period of two years but it may thereafter transfer such competence to the National Data Management Office (NDMO).

The Law will come into effect on 23 March 2022, at which time the Data Authority will be required to issue the Law's implementing regulations ("**Regulations**"). Controllers (as defined below) will have one year from the effective date to comply with the Law.

The introduction of the Law is a significant development in Saudi Arabia's legislative landscape that will have implications on almost all entities operating in the market or who offer their services to Saudi customers. Before its introduction, 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.

Below we provide an overview and the most notable features of the Law.

Scope and application

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

The Law will regulate (1) processing that takes place in Saudi Arabia, and (2) processing of the Personal Data of a Saudi resident that takes place outside of Saudi Arabia. The majority of the Law's requirements are imposed on the entity that determines the manner and purpose of the processing ("**Controller**").

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

- it grants mandatory rights to Data Owners over their Personal Data;

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

Personal Data

As an example only, Personal Data may include an individual's name, personal identification numbers, records, photos and videos of the individual.

The Law also identifies a sub-category of Personal Data of a more sensitive nature that must be afforded a greater degree of protection ("**Sensitive Data**"). This includes Personal Data that includes a reference to an individual's:

- ethnic or tribal origin;
- religious, intellectual or political beliefs;
- membership in civil associations or institutions;
- criminal and security data;
- bio-identifying and genetic data;
- health data;
- credit data;
- location data; and
- data that indicates that one or both of the individual's parents are unknown.

Data Owners' consent

A Data Owner's prior consent is required to process their Personal Data unless one of the following alternative grounds to legitimize processing applies:

- the processing achieves a "real interest" for the Data Owner and communication with them is impossible or difficult;
- the processing is being conducted pursuant to another law or in implementation of a previous agreement with the Data Owner; or
- the Controller is a government entity and the processing is required for security purposes or to satisfy judicial requirements.

Additionally, Personal Data may be collected or processed without the Data Owner's consent for scientific, research or statistical purposes if it is anonymized or if it is being collected or processed pursuant to another law or in implementation of a previous agreement with the Data Owner.

Data Owners are entitled to withdraw their consent to the processing of their Personal Data at any time and the Regulations will set out further details relating to the exercise of this right.

The Law stipulates that a service or benefit offered to a Data Owner must not be conditional on their consent to certain processing, unless the processing is related to the service or benefit they are receiving. The Law does not stipulate what form or standards the consent obtained must meet. More details will be set out in the Regulations.

Linked to the critical subject of consent is the default assumption under the Law that the Controller should collect Personal Data directly from the relevant Data Owner. The Controller may only collect Personal Data from a person other than the Data Owner in the following circumstances (to be further detailed in the Regulations):

- the Personal Data Owner agrees to such collection;
- the Personal Data is publicly available, or collected from a publicly available source;
- the Controller is a government entity and such collection is for security purposes or to satisfy judicial requirements;
- the Data Owner's vital interests would be harmed if their Personal Data is not collected from such other person;
- the collection of Personal Data is necessary to protect public health or safety, or to protect the life or health of a specific individual; or
- the Personal Data is anonymized.

Personal Data protection principles

Below are an overview of the Personal Data protection principles provided for under the Law:

- **Purpose limitation:** the Personal Data should only be processed for the purpose for which it was originally collected, subject to the Data Owner's consent to any change to those purposes, or unless one of the circumstances set out above applies.
- **Relevance:** the type of Personal Data collected must be appropriate and limited to the minimum necessary to achieve the purpose of its collection.
- **Accurate, complete and up-to-date:** the Controller should not process Personal Data without verifying its accuracy, completeness, timeliness and relevance for the underlying purpose.
- **Fairness and transparency:** the method by which Personal Data is collected must be direct, clear and secure, and not entail deception, misleading actions or blackmail.
- **Kept for no longer than is necessary:** once the Personal Data is no longer necessary to achieve the purpose, the Controller must cease its collection and destroy the data previously collected (subject to a right to retain it where a legal justification exists for a specific period, or if it the Personal Data closely relates to a judicial proceeding until such proceeding has concluded).

Controller's obligations

The Law imposes certain obligations on Controllers, including the following:

- **Fair processing notification:** Controllers must inform Data Owners of:
  - the legal or practical justification for collection;

- the 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);
- the Controller's identity and address; and
- the entity or entities to which the Personal Data will be disclosed, their capacity, including will be transferred, disclosed, or processed outside of Saudi Arabia.

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 Law.

We note that much of this information would customarily be included in a privacy policy, presentation of which is identified as a separate requirement under the Law.

- **Privacy policy:** Controllers must adopt and present a privacy policy to Data Owners for review prior to collecting their Personal Data. The privacy policy must at a minimum specify:
  - the purpose of collection;
  - the nature of the Personal Data to be collected;
  - the collection and storage method and the means of processing;
  - the manner by which the Personal Data will be destroyed; and
  - the rights of Data Owners, 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 transfer, in accordance with the provisions set out in the Regulations.
- **Data privacy impact assessments:** Controllers must conduct an evaluation of the effects of processing associated with any product or service provided to the public, in accordance with the requirements of the Regulations.
- **Data breach reporting:** Controllers must notify the Data Authority as soon as they become aware that Personal Data has been leaked, damaged or illegally accessed. The Regulations will specify the instances when the Data Owner must also be informed of a security breach affecting their Personal Data.
- **Data officer:** Controllers must appoint or assign at least one of their employees to be responsible for achieving compliance with the Law.
- **Destruction of Personal Data:** as noted in the principles section above, 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 conditions set out in the Regulations.
- **Record of processing:** without prejudice to the requirements relating to Personal Data destruction, Controllers must maintain a record of processing activities for a period to be specified by the Regulations to be made available to the Data Authority upon request, and must include the purpose of the processing, entities to which the Personal Data was or will be disclosed, whether the Personal Data was or will be transferred outside of Saudi Arabia and the expected retention period.

- **Employee seminars:** after 23 March 2022, Controllers will be required to hold seminars for their employees to familiarize them with the principles of the Law.

Cross-border Personal Data transfers

The Law generally prohibits Controllers from transferring Personal Data outside of Saudi Arabia or disclosing Personal Data to an entity outside of Saudi Arabia, except where:

- the transfer or disclosure will not adversely affect the national security or the vital interests of the Kingdom;
- sufficient guarantees are provided to safeguard the data transferred or disclosed and to protect the confidentiality of the same and that they meet the minimum criteria stipulated in the Regulation
- the Personal Data is exported is limited to the minimum amount necessary; and
- consent of the Data Authority has been obtained in respect of the transfer or disclosure concerned.

Data Owners' rights

The Law grants certain rights to Data Owners in respect of their Personal Data, including the following:

- **Right to be informed:** the right to be informed of the legal or practical justification and purpose for collecting their Personal Data.
- **Right to access:** the right to receive a copy of their Personal Data held by the Controller free of charge (except for fees required to obtain credit data under the Credit Information Law). Notably the Law provides for certain restrictions and exceptions to this right, including where providing the Personal Data to the Data Owner would be detrimental to the public interest or detrimental to national or public security.
- **Right to rectification:** the right to rectify, supplement or update their Personal Data held by the Controller and the Controller must notify any party to whom the Personal Data has been transferred of the rectification.
- **Right to destruction:** the right to request the destruction of their Personal Data held by the Controller, subject to the Controller's ability to anonymize it to prevent identification of the Data Owner and subject to any legal justification or court proceedings that mean that it needs to be retained.

The Controller is obliged to respond to requests within the time period and in accordance with the stipulations to be specified in the Regulation. It is also worth noting that additional rights may be afforded to the Data Owner in the Regulations.

Controller registry

The Data Authority intends to establish a national registry of Controllers. All Controllers will be required to register through a publicly available portal and Controllers who are private entities or private individuals will be required to pay an annual fee of a maximum of SAR 100,000.

Categories of data that will be subject to further regulation

Additional controls and procedures will be introduced for the processing of health data and credit data. These further controls and procedures will not contradict the requirements of the Law.

Penalties

The potential penalties for violations of the Law are:

- imprisonment of up to two years and/or a fine up to SAR 3,000,000 for anyone who discloses or publishes Sensitive Data in violation of the Law;
- imprisonment of up to one year and/or a fine up to SAR 1,000,000 for anyone who violates the general prohibition on transfers of Personal Data outside Saudi Arabia; and
- a warning or fine up to SAR 5,000,000 for any other violations of the Law, which fine may be doubled if repeated.

Contact us

Abdulrahman AlAjlan
abdulrahman.alajlan
@legal-advisors.com

Zahi Younes
zahi.younes
@legal-advisors.com

Yousef Bugaighis
yousef.bugaighis
@legal-advisors.com

Kellie Blyth
kellie.blyth
@bakermckenzie.com