Bahrain Publishes Personal Data Protection Law

17 SEP 2018
By: Mohamed Toorani | Eamon Holley

On 12 July 2018, the Kingdom of Bahrain (Bahrain) issued Law No. 30 of 2018 on the Personal Data Protection Law (PDPL). The PDPL will enter into force on 1 August 2019, giving businesses just under one year from the date of this article to prepare for the new regime.

The PDPL will be a paradigm shift for how business is done in Bahrain. It will provide individuals with rights in relation to how their personal data can be collected, processed and stored. Conversely, it will impose new obligations on how businesses manage this, including ensuring that personal data is processed fairly, that data owners (often referred to as “data subjects” in other data protection laws) are notified of when their personal data is collected and processed and that data owners can exercise their rights directly with the businesses.

The PDPL also imposes new obligations upon businesses to ensure that the personal data they collect is kept secure.

The PDPL will set up a new authority, known as the Personal Data Protection Authority (Authority). This Authority has the power to investigate allegations of violations of the PDPL either by itself, at the request of the responsible Minister, or in response to a complaint.

The Authority can issue orders to stop violations, including issuing emergency orders and fines. Civil compensation is also allowed for any individual who has incurred damage arising from the processing of their personal data by the data manager (often referred to as a “data controller” in other data protection laws), or violating the provisions of the PDPL by a business's data protection supervisor (often referred to as a “data protection officer” in other data protection laws). Finally, the most concerning feature of this law for businesses is that the PDPL carries criminal penalties for violations of certain provisions.

While the PDPL can be compared to laws such as the European Union's General Data Protection Regulation (GDPR), there are important differences that need to be considered. Businesses operating in Bahrain that have recently implemented a GDPR compliance program will still need to pay close attention to these differences and should be aware of the new obligations in the PDPL.

In this article we review some of the main features of this new law.

APPLICATION

The PDPL applies to:

- Individuals normally residing or having a workplace in Bahrain
- Businesses with a place of business in Bahrain; and
- Individuals not normally residing or having a workplace in Bahrain, and businesses not having a place of business in Bahrain, but processing personal data by using means available in Bahrain, unless the use of such
processing means are solely for the purpose of passing data through Bahrain without any other purpose

In the last scenario, each business must appoint a local representative in Bahrain to carry out its obligations and notify the Authority of that appointment. The PDPL will therefore have extra-territorial effect. If an individual or business not in Bahrain is processing personal data within Bahrain through means such as their appointed local representatives, the PDPL would apply.

REGULATION

Personal data is defined as any information of any form related to an identifiable individual, or an individual who can be identified, directly or indirectly, particularly through their personal identification number, or one or more of their physical, physiological, intellectual, cultural or economic characteristics or social identity.

Sensitive personal data is a subset of personal data. It is personal data which reveals, directly or indirectly, the individual's race, ethnicity, political or philosophical views, religious beliefs, union affiliation, criminal record or any data related to their health or sexual life. Sensitive personal data requires more rigorous treatment by data managers.

Processing is defined as any operation or set of operations carried out on personal data by automated or non-automated means, such as collecting, recording, organising, classifying in groups, storing, modifying, amending, retrieving, using or revealing such data by broadcasting, publishing, transmitting, making them available to others, integrating, blocking, deleting or destroying them.

Like the GDPR, the PDPL requires that personal data:

- Is processed fairly and legitimately
- Is collected for a legitimate, specific and clear purpose
- Is sufficient, relevant and not excessive for the purpose of the data's collection or for the purpose for which subsequent processing is carried out
- Is correct and accurate, and subject to updates whenever necessary; and
- Shall not remain in a form allowing identification of the data owner after meeting the purpose of its collection or for the purpose for which subsequent processing is carried out. The PDPL does allow the storage of anonymised data for a longer time for historical, statistical or scientific research purposes

PROCESSING

Processing of personal data can only occur with the consent of the data owner, unless the processing is necessary:

- To implement a contract to which the data owner is a party
- To take steps at the request of the data owner to conclude a contract
- To implement an obligation required by law, contrary to a contractual obligation or an order from a competent court
- To protect the vital interests of the data owner; or
- To exercise the legitimate interests of the data manager or any third party to whom the data is disclosed, unless this conflicts with the fundamental rights and freedoms of the data owner

Processing of sensitive personal data is also prohibited without the consent of the data owner, unless one of the exceptions in Article 5 of the PDPL apply.

However, it is prohibited for data managers to process the following personal data types without the prior written authorisation of the Authority:

- Automatic processing of sensitive personal data of persons who cannot provide consent
- Automatic processing of biometric data
- Automatic processing of genetic data (except for treatment provided by physicians and specialists at a licensed medical establishment, where the treatment is necessary for purposes of preventative medicine or diagnostic medicine, or for the provision of treatment or healthcare)
• Automatic processing that entails the connection of personal data files that are in the possession of two or more data managers that are processing personal data for different purposes; and
• Processing that consists of visual recording to be used for monitoring purposes

CONSENT

Like the GDPR, the PDPL has specific requirements about how consent must be given. For consent to be valid it must be:

• Issued by an individual of full eligibility
• Written, explicit and clear; and
• Issued based upon the data owner's free will and consent, after being fully informed about the purposes of the processing of their personal data

The data owner has a right to withdraw consent at any time. The Authority's Board of Directors must issue a resolution outlining these procedures for withdrawing consent and the data manager's decision on requests for withdrawal of consent.

RIGHTS OF DATA OWNER

The PDPL introduces several concepts that data managers will need to become very familiar with. Again, those familiar with the GDPR will see similarities here with the GDPR's data subject rights.

Where the data is collected, directly or indirectly, from the data owner, the data manager at the time of registering such data, must notify the data owner of the following information:

• The full name of the data manager, their field of activity or profession and address
• The purpose for which the data is to be processed
• Names or categories of the recipients of the data
• Details about the data owner's rights in respect of the data; and
• Whether the data will be used for direct marketing

This notification is important, because it alerts data owners of their rights regarding their personal data. These rights include:

• To be notified of when their data is being processed
• To object to direct marketing
• To object to processing that causes harm or distress to data owner or others
• To object to decisions made based upon automated processing; and
• To rectify, block or erase personal data in certain circumstances

SECURITY

The PDPL requires that data managers apply technical and organizational measures capable of protecting the data against unintentional or unauthorized destruction, accidental loss, unauthorized alteration, disclosure or access, or any other form of processing.

The PDPL requires that the Authority's Board of Directors issues a decision specifying the terms and conditions that the technical and organizational measures must satisfy. The decision may require specific activities by applying special security requirements when processing personal data.

Data managers must also use data processors who will provide sufficient guarantees about applying the technical and organizational measures that must be adhered to when processing the data. Data managers must also take reasonable steps to verify that data processors comply with these measures.

Interestingly, there is no mandatory data breach notification provision in the PDPL requiring the data managers to notify the Authority or data owner in the event that there is a breach of personal data held by the data manager.
TRANSFERS OF PERSONAL DATA OUTSIDE OF BAHRAIN

Transfers of personal data out of Bahrain is prohibited unless the transfer is made to a country or region that provides sufficient protection to personal data. Those countries need to be listed by the Authority and published in the Official Gazette.

Data managers can also transfer personal data to countries that are not determined to have sufficient protection of personal data where:

- The data owner has consented to the transfer
- The data is from a public register
- The transfer is necessary for:
  - Executing a contract between the data owner and data manager, or taking preceding steps at the data owner's request for the purpose of concluding the contract
  - Executing or concluding a contract between the data manager and a third party for the benefit of the data owner
  - Protecting the data owner's vital interests
  - Fulfilling a non-contractual obligation imposed by law, or an order of the court, public prosecution, an investigating judge or military prosecution; or
  - Preparing, executing or defending a legal claim

Transfers can also be made with the permission of the Authority, issued on a case-by-case basis, if it deems that the data will be sufficiently protected.

APPOINTMENT OF A DATA PROTECTION SUPERVISOR

Data managers may voluntarily appoint a data protection supervisor. The Authority's Board of Directors may also issue a decision requiring specific categories of data managers to appoint data protection supervisors. However, in all instances, the data manager must notify the Authority of such an appointment within three (3) days of its occurrence.

A data protection supervisor must help the data manager in exercising its rights and fulfilling its obligations prescribed under the PDPL. The data protection supervisor also has a number of other roles, including liaising with the Authority, verifying that personal data is processed in accordance with the PDPL, notifying the Authority of any violations of the PDPL that the supervisor becomes aware of and maintaining a register of processing operations that the data manager must notify the Authority about.

The Authority must create a register of data protection supervisors. To be accredited as a data protection supervisor, an individual must be registered in that register.

ORDERS, CIVIL, COMPENSATION AND CRIMINAL PENALTIES

The Authority can issue orders to stop violations, including emergency orders and fines. Civil compensation is also allowed for any individual who has incurred damage arising from the processing of their personal data by the data manager, or arising from the data protection supervisor's violation of the PDPL. Appeals can be made against decisions of the Authority.

Finally, the PDPL also carries a range of criminal penalties and administrative fines for violating certain provisions.

Criminal penalties of imprisonment of not more than one (1) year and/or a fine between BHD 1,000 (circa US$ 2,645) to BHD 20,000 (circa US$ 52,910), can be issued against any individual who:

- Processes sensitive personal data in violation of the PDPL
- Transfers personal data outside Bahrain to a country or region in violation of the PDPL
- Processes personal data without notifying the Authority
- Fails to notify the Authority of any change made to the data of which they have notified the Authority
- Processes certain personal data without prior authorization from the Authority
• Submits to the Authority or the data owner false or misleading data to the contrary of what is established in the records, data or documents available at their disposal
• Withholds from the Authority any data, information, records or documents which they should provide to the Authority or enable it to review them in order to perform its missions specified under the PDPL
• Causes to hinder or suspend the work of the Authority’s inspectors or any investigation which the Authority is going to make; and/or
• Discloses any data or information which he is allowed to have access to due to his job or which he used for his own benefit or for the benefit of others unreasonably and in violation of the provisions of the PDPL

NEXT STEPS

Businesses that have already implemented a data protection compliance program under the GDPR may have developed some of the infrastructure that will apply under the PDPL; however compliance with the GDPR will not guarantee compliance with the PDPL. For example, businesses that are data managers will need to:

• Recognise the right of Bahraini data owners to object to processing of personal data that causes harm or distress to the data owner or another person (this is not a data subject right found in the GDPR)
• Notify the Authority of their processing; and
• Obtain prior written approval of the Authority to process certain types of personal data (this is not found in the GDPR)

Finally, the risk of criminal penalties is a risk that is not found in the GDPR (although it is possible that Member States of the European Union may have specific laws that may be similar).

As a first step, a business will need to determine if its activities mean that it falls within the definitions of data manager. If it does, then it will need to determine what sort of personal data it is collecting, from who, and for what purposes. Data managers need to ensure that they are collecting and processing personal data and, in particular, sensitive personal data, in accordance with the PDPL, including notifying the Authority of their processing activities, or preparing submissions for permission to process certain types of personal data.

DLA Piper’s Middle East data protection team has deep experience in assisting clients in assessing their data protection compliance risks, and developing remediation and compliance programs.

Although the PDPL will become effective on 1 August 2019, our experience with the GDPR has shown us that data mapping exercises are often complex and resource intensive exercises. Early preparation for commencement of the PDPL will pay off in the longer term.

For more information or to discuss how this may affect you, please contact Mohamed Toorani or Eamon Holley.

AUTHORS

Mohamed Toorani
Legal Director
Manama | T: +973 1755 0890
[email protected]

Eamon Holley
Partner
Dubai | T: +971 4 438 6100
[email protected]