Akin®

Bahrain's New Data Protection Law Now in Force

Aug 20, 2019

Reading Time : **4 min**

By: Natasha G. Kohne, Mazen Baddar

Bahrain's adoption of the PDPL may be part of a trend among members of the Gulf Cooperation Council (GCC) toward increased data protection oversight. The United Arab Emirates and Saudi Arabia, for example, may both introduce more comprehensive data protection laws in the coming years[1].

The PDPL includes criminal penalties for certain violations. Data protection laws in the European Union and the United States, in contrast, are generally civil in nature. Criminal violations include the processing of sensitive personal data in contravention of the PDPL or withholding data, information, records or documents requested by the Authority.

The law applies to individuals living and working in Bahrain; organizations with a place of business in Bahrain; and people and organizations that are not present in Bahrain but that process data using means (independently or through third parties) available in Bahrain, unless such processing is solely for the purpose of passing data through Bahrain. The law follows a somewhat analogous dichotomy to the European Union's General Data Protection Regulation (GDPR) in defining two main roles with regard to data: (1) data manager, the person who decides (solely or in conjunction with others) the purposes and means of processing; and (2) data processor, the person who processes the data for and on behalf of the data manager.

The collection, processing and transfer of data or personal data and sensitive personal data is protected by the PDPL. Different restrictions apply to the different categories of information. "Data or personal data" is defined as information in any form that is related to an identifiable individual or an individual who can be identified, directly or indirectly, through an identifying factor (e.g., personal ID number, physical, cultural or economic factors). "Sensitive

personal data" is a subset of personal data that reveals, directly or indirectly, an individual's race, ethnicity, political or philosophical views, religious beliefs, union affiliation, criminal record or any data related to his or her health or sexual life. The PDPL more rigorously regulates the processing of sensitive personal data; for example, sensitive personal data may not be processed using automated means.

The PDPL defines "processing" as the carrying out of any operation or set of operations on personal data whether that processing is automated or not. Processing broadly includes, for example, organizing, collecting, storing, retrieving or revealing personal data.

Certain consent restrictions apply to the processing of data under the PDPL. An organization generally must have the consent of the owner of the personal data to process the data. Consent must be (1) written, explicit and relate specifically to the processing of specific data; (2) freely given; and (3) fully informed regarding the intended purpose. The data owner retains the right to withdraw his/her consent at any time. However, there are certain limited exceptions to the requirement for consent, including where the processing is necessary for the implementation of a contract to which the data owner is a party.

In addition, processing certain data is prohibited without first obtaining the prior written authorization of the Authority. For example, the Authority's prior written authorization is required when automatically processing sensitive personal data or biometric data used for identification purposes, such as thumb prints used on many smart phones. The PDPL prohibits the transfer of personal data out of Bahrain unless it is transferred to a country the Authority includes on its list of approved countries (the "List"). The List, when published, will consist of countries that, in the view of the Authority, have sufficient personal data protections. Transfers to countries that are not on the List are permitted in limited circumstances, for example, where the data owner provides consent or the data was obtained from a public source.

Violation of the PDPL can lead to either civil or criminal liability, depending on the circumstances. With regard to civil public enforcement, the Authority may place a stop order on the collection, processing or transferring of personal data. Stop orders may lead to delays and inconveniences for businesses. The Authority may also impose administrative fines of up to 20,000 BD (approximately $53,000). Individual data owners who have suffered a loss as a result of a violation of the PDPL may bring a civil complaint in the Bahraini courts to seek

compensation from the offender. Criminal prosecution may lead to imprisonment for up to one year and/or the imposition of criminal fines of up to 20,000 BD (approximately $53,000).

The PDPL introduces a broad range of new obligations for those who operate within Bahrain or process data using means available in Bahrain. To minimize the risk of liability, covered persons and entities should act now to ensure they are compliant with the law. The following are practical steps to assist with compliance:

- Determine if you are using means, whether independently or through third parties, available in Bahrain to process personal data.
- Understand how you process data and seek the consent of the data owner prior to processing, or the prior written authorization of the Authority where required (for example, when automatically processing sensitive or biometric data).
- Determine whether you are processing personal data and/or sensitive personal data and whether you have sufficient protections in place to meet the different restrictions on the processing of both types of personal data.
- If you have not done so already, establish a role within your organization to coordinate, monitor and regularly update your data protection program. If the role exists, ensure those responsible are aware of the new PDPL requirements.

[1] See, e.g., TechRadar, Privacy regulators in GCC countries get more muscles to flex (Aug. 3, 2019), available at: https://www.techradar.com/news/data-privacy-regulators-in-gcc-countries-get-more-muscles-to-flex.

Categories

Cybersecurity, Privacy & Data Protection | Asia | GDPR

Federal Privacy Policy