DATA PROTECTION LAWS OF THE WORLD

Bahrain

DLA PIPER

Downloaded: 10 May 2024

BAHRAIN

Last modified 17 January 2024

LAW

Bahrain enacted Law No. 30 of 2018 with respect to Personal Data Protection ("**PDPL**") on July 12, 2018. The PDPL is the main data protection regulation in Bahrain. The PDPL came into force on August 1, 2019, and supersedes any law with contradictory provisions. On March 17, 2022, the Personal Data Protection Authority ("**Authority**") has issued 10 ministerial resolutions supplementing the PDPL ("**Resolutions**"). The Resolutions cover the following:

1. duties of the Data Protection Officer and related fees;
2. technical and organisational measures;
3. notification procedures;
4. rules regarding data processing;
5. rules regarding processing of sensitive personal data;
6. rules regarding data subject rights;
7. rules regarding how public registers must treat personal data;
8. rules regarding data relating to criminal proceedings;
9. rules regarding making complaints to the Authority; and
10. rules regarding the transfer of personal data outside Bahrain.

DEFINITIONS

Definition of personal data

Personal data is defined under the PDPL 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.

Definition of sensitive personal data

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 controllers.

NATIONAL DATA PROTECTION AUTHORITY

Under the PDPL, the Authority will have power to investigate violations of the PDPL on its own, 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 controller, or violating

the provisions of the PDPL by a business's data protection officer. Finally, the most concerning feature of the PDPL for businesses is that it carries criminal penalties for violations of certain provisions.

Decree No. 78 of 2019 (the " **Decree**") was enacted to determine the administrative authority that will assume the mandated functions and powers of the Authority. This Decree came into force September 29, 2019.

Article I of the aforementioned Decree appoints the Ministry of Justice, Islamic Affairs and Endowments (the " **Ministry**") as the Authority for the protection of personal data in accordance with the provisions of the PDPL, on a temporary basis pending the financial allocation of the Authority in the general budget of Bahrain and the issuance of a decree forming the Board of Directors pursuant to Article 39 of the PDPL.

The Minister of the Ministry will assume the functions and powers prescribed to Board of Directors of the Authority and the Chairman of Board of Directors, in accordance with the provisions of the PDPL The Undersecretary of the Ministry will assume the same functions and powers as the Executive Chairman.

REGISTRATION

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

DATA PROTECTION OFFICERS

Data controllers may voluntarily appoint a data protection officer. The Authority's Board of Directors may also issue a decision requiring specific categories of data controllers to appoint data protection officers. However, in all instances, the data controller must notify the Authority of such an appointment within three days of its occurrence.

A data protection officer must help the data controller in exercising its rights and fulfilling its obligations prescribed under the PDPL The data protection officer 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 data protection supervisor becomes aware of and maintaining a register of processing operations that the data controller must notify the Authority about.

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

COLLECTION & PROCESSING

Processing is defined under the PDPL as any operation or set of operations carried out on personal data by automated or non-automated means, such as collecting, recording, organizing, 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.

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

- to implement a contract to which the data subject is a party;
- to take steps at the request of the data subject 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 subject; or
- to exercise the legitimate interests of the data controller or any third party to whom the data is disclosed, unless this conflicts with the fundamental rights and freedoms of the data subject.

Processing of sensitive personal data is also prohibited without the consent of the data subject, except when the processing:

- is required by the data controller to carry out their obligations;
- is necessary for the protection of the data subject;
- of the data is made available to the public by the data subject;

- is necessary to exercise any of the procedures of claims of legal rights or the defence thereof;
- is necessary for the purposes of preventive medicine, medical diagnosis, provision of healthcare, treatment or management of healthcare services;
- is carried out within the activities of associations, unions and other non-profit organisations;
- is carried out by a competent public entity; or
- is related to the race or ethnicity, if they are necessary to ascertain equal opportunities or treatment of the society's individuals.

Data controllers are prohibited from processing the following personal data types without the prior written authorization of the Authority:

- automatic processing of sensitive personal data of data subjects who cannot provide consent;
- automatic processing of biometric data;
- automatic processing of genetic data (unless such processing was provided by physicians and specialists at a licensed medical establishment and is necessary for purposes of preventative medicine or diagnostic medicine, or purposes to provide treatment or healthcare);
- automatic processing of personal data files that are in the possession of two or more data controllers that are processing personal data for different purposes; or
- processing that consists of visual recording to be used for monitoring purposes.

TRANSFER

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. The Authority has listed the countries in which it deems provides adequate regulatory and legislative protection for personal data. Data controllers would be permitted to transfer personal data directly to the states, countries and territories listed in the regulation, without obtaining prior authorization from the Authority. The list of 83 countries are as follows:

- Andorra, Bulgaria, Denmark, French Guiana, Iceland, Argentina, Canada, Ecuador, Georgia, India, Australia, Chile, Egypt, Germany, Ireland, Austria, China, Estonia, Greece, Isle of Man, Belgium, Colombia, Falkland Islands, Guernsey, Israel, Bolivia, Croatia, Faroe Islands, Guyana, United Kingdom, Brazil, Cyprus, Finland, Hong Kong, Italy, Brunei, Czech Republic, France, Hungary, Japan, Luxembourg, Nigeria, Russia, Switzerland, Jersey, Macau, Norway, San Marino, Thailand, Jordan, Malaysia, Oman, Singapore, Ukraine, Kazakhstan, Malta, Pakistan, Slovakia, United Arab Emirates, Kingdom of Saudi Arabia, Mexico, Paraguay, Slovenia, United States of America, Kuwait, Monaco, Peru, South Korea, Uruguay, Latvia, Morocco, Poland, Spain, Vatican, Liechtenstein, Netherlands, Portugal, Suriname, Venezuela,Lithuania, New Zealand, Romania and Sweden.

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

- the transfer occurs pursuant to a permission to be issued by the Authority on a case-by-case basis, if it deems that the
- data will be sufficiently protected;
- if the data subject has consented to that transfer;
- if the data to be transferred has been extracted from a register that was created in accordance with the PDPL for the purpose of providing information to the public, regardless of whether viewing of this register is available to everyone or limited to the parties concerned in accordance with specific terms and conditions. In this instance, one shall have to satisfy the terms and conditions prescribed for viewing the register before viewing that information;
- if the transfer is necessary for any of the following:
    - to implement a contract between the data subject and the data controller, or to undertake preceding steps at the data subject's request for the purpose of concluding a contract;
    - to implement or conclude a contract between the data controller and a third party for the benefit of the data subject;
    - to protect the data subject's vital interests;

- to implement an obligation imposed by the PDPL (even if this is contrary to the contractual obligation), or to implement an order issued by a competent court, the public prosecution, the investigating judge or the military prosecution; or
- to prepare, execute or defend a legal claim.

SECURITY

The PDPL requires that data controllers 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 controllers 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 controllers must also take reasonable steps to verify that data processors comply with these measures.

BREACH NOTIFICATION

The data controller shall establish specific procedures to inform the Personal Data Protection Authority of the occurrence of any violation or breach of data within a period not exceeding (72) hours from the date of its discovery, unless if the such personal data breach would not affect the rights of data subjects.

ENFORCEMENT

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 controller, or arising from the data protection officer's violation of the PDPL Appeals can be made against decisions of the Authority.

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 year and / or a fine between BHD 1,000 to BHD 20,000, 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 subject 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 they are allowed to have access to, due to their job or which they used for their own benefit or for the benefit of others unreasonably and in violation of the provisions of the PDPL.

ELECTRONIC MARKETING

Under the PDPL, data controllers must notify the data subject when data is collected directly or indirectly of whether data will be used for direct marketing purposes. Notice is important because it alerts data subjects of their right to object to any direct marketing relating to their personal data.

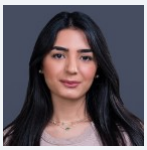
ONLINE PRIVACY

There is no specific online privacy regulation in Bahrain.

KEY CONTACTS

Mohamed Toorani
Legal Director - Head of Bahrain Office
T +973 1 755 0896
mohamed.toorani@dlapiper.com

Lulwa Alzain
Associate
T +973 1 755 0891
lulwa.alzain@dlapiper.com



Jenan Banahi
Associate
T +973 1755 0897
jenan.banahi@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.