BAHRAIN DATA PROTECTION OVERVIEW

AUTHORS

FATIMA ALALI
PARTNER

HASSAN ALKOOFI
ASSOCIATE

HASSAN RADHI & ASSOCIATES
www.hassanradhi.com
info@hassanradhi.com

ERA BUSINESS CENTRE
P.O.Box: 5366
Building 361, Road 1705, Block 317
Kingdom of Bahrain

A LexMundi Member

1. THE LAW

1.1. Key Acts, Regulations, Directives, Bills (only if highly likely to become law)

Data protection in the Kingdom of Bahrain is mainly governed by Law No. 30 of 2018 Promulgating Personal Data Protection Law (the "Data Protection Law") which was recently announced in the official gazette of 19-07-2018.

Prior the enactment of the Data Protection Law, Bahrain had certain provisions in other legislation which govern the concept of data protection. The aforementioned provisions remain enforceable and serve as supplementary provisions to the Data Protection Law and regulate the concept of data protection in specific sectors, such as:

• Central Bank of Bahrain and Financial Institutions Law 2006, which regulates data protection in the regulated financial activities sector.

• Legislative Decree No. 48 of 2002 promulgating the Telecommunications Law, which regulates data protection in the telecommunication sector.

• Labour Law, which regulates data protection in employee-employer relationships.

Nonetheless, the Data Protection Law serves as the main piece of legislation with respect to data protection issues, and therefore this note will focus on the implications of the Data Protection Law.

It is worth noting that the Data Protection Law was recently enacted, therefore many procedural and regulatory issues covered in the Data Protection Law which are to be decided by way of resolution by the Authority are yet to be issued.

2. SCOPE OF APPLICATION

2.1. Who do the laws/regs apply to?

The provisions of the Data Protection Law apply to any natural person who resides normally in Bahrain or has a place of business in Bahrain, any legal person who has a place of business in Bahrain and any natural or legal person who processes data using the means available in Bahrain, unless the purpose of using data processing means in Bahrain is to pass the data on to a different jurisdiction through Bahrain.

2.2. What types of processing are covered/exempted?

The Data Protection Law sets out the types of processing that fall within the scope of its application as follows:

- the processing of data using automatic means in whole or in part; and
- the processing of data that forms or is intended to form part of a file system by a non-automatic means.

The following data is expressly excluded from the scope of application of the Data Protection Law:

- the processing of data made by any individual for purposes not exceeding personal or family affairs; and
- data processing done by the security services of Bahrain for the purposes of national security.

In addition, the Data Protection Law specifies that the application of the provisions thereof shall not in any case prejudice the requirements of confidentiality required in connection with the affairs of the Bahrain Defense Force.

3. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

3.1. Main regulator for data protection

The main regulatory authority for data protection in Bahrain is the Personal Data Protection Authority (the "Authority"), which shall be established pursuant to Article (27) of the Data Protection Law.

3.2. Main powers, duties and responsibilities

The main duties and responsibilities of the Authority pursuant to the Data Protection Law include:

- Issuing the decisions necessary for the implementation of the Data Protection Law such as and without limitation, specifying the (i) rules and procedures that data controllers must comply with in respect of data processing ;(ii) technical and organizational standards that must be met by data controllers; and (iii) conditions of data record keeping.
- Authorizing the transfer of data outside the Kingdom of Bahrain.
- Assessing, approving or denying any notifications/applications received for the commencement of data processing.
- Maintaining a register for the permits issued or notifications received for the commencement of data processing.
- Receiving complaints with regards to any violation of the provisions of the Data Protection Law
- Educating the public and data controllers with their rights and obligations pursuant to the Data Protection Law
- Monitoring the compliance with the provisions of the Data Protection Law.
- Supervising and inspecting data controllers regarding processing personal data.
- Supervising and inspecting the work of data protection officers in order to verify their compliance with the provisions of the Data Protection Law.
- Examine the legislation relating to the protection of personal data and recommend their amendment in accordance with internationally recognized standards.
- Raising awareness with regards to data protection by organizing educational training and promoting personal data protection culture.
- Represent Bahrain in international conferences as the body responsible for the protection of personal data

Provided that the Data Protection Law is still in the implementation phase, a decree is yet to be issued to specify the duties and powers vested in the administrative body of the Personal Data Protection Authority.

4. KEY DEFINITIONS | BASIC CONCEPTS

The key terms which were defined under Article (1) of the Data Protection Law are the following:

Authority: The Personal Data Protection Authority

Personal Data : Any information, in any form, of an identified, directly or indirectly identifiable, individual particularly through his/her personal identification number or one or more of his/her formal, physiological, intellectual, cultural, economic or social identity.

To determine whether an individual is capable of being identifiable or not, all means used by, or which may be available to, data controller or any other person shall be taken into consideration.

Sensitive Personal Data: Any personal information that directly or indirectly discloses the individual's ethnic or racial origin, political or philosophical opinions, religious beliefs, trade union affiliation, criminal record, or any data relating to his/her health or sexual status.
Data Controller: A person who, either alone or jointly or in common with other persons, determines the purposes and means of the processing of certain personal data. Where such purposes and means are established by law, the person responsible for the obligation to perform processing shall be data controller.
Data Processor: Any person, other than an employee of the data controller or data processor, who processes the data for and on behalf of the data controller.
Processing: Any process or a set of processes carried out on personal data through automatic or non-automatic means, including the collection, recording, organization, classification, storage, adaptation or alteration, retrieval, use or disclosure of such data by transmission, dissemination or otherwise making available, combination, blocking, erasure or destruction of the information or data.

5. NOTIFICATION | REGISTRATION

5.1 Requirements and brief description

5.1.1 NOTIFICATION

The Data Controller is required to notify the Authority before the commencement of any data processing, and the notifications received will be entered into the "register of notifications and permits" which is maintained by the Authority.
The Authority will issue a decision to specify the procedures and regulations in connection with the notice, nonetheless, the notice shall contain the following information:
a. the name and address of the data controller and the data processor;
b. the purpose of processing;
c. data description and statement of categories of data subjects and recipients of these data or their categories;
d. any transfer of data to a country or territory outside the Kingdom, intended to be carried out; and
e. a statement that enables the Authority to assess in principle the appropriateness of the measures available to meet the safety requirements (outlined under paragraph 6 below).

The Data Controller may be exempted from the notification requirement in the following circumstances:
a. where the sole purpose of data processing is to maintain a record in accordance with the law in order to provide information to the public, whether access to the information is available to the public as a whole or limited to concerned parties;
b. processing of data in the context of the activities of associations of all kinds, trade unions and other non-profit organizations;
c. where an employer is processing the data of his/her employees within the limits necessary to carry out its functions related to the employment, organize the employees' employment affairs, exercise the rights outlined under the Labour Law with respect to data processing data and protect the rights of the employees;
d. in cases where a data protection officer is appointed (as explained in paragraph 10 below).

The Authority may contact the data controller within 10 days of the receipt of the notification in order to request the data controller to complete any shortfall in the

information contained in the notice. Such shortfall is required to be remedied within 15 days from the date of such request, and the data controller shall be required to stop processing the data until the shortfall in information is completed.
Any uncompleted notification that was not completed after receiving the request outlined above may be struck off from the Authority's register by virtue of a reasoned decision issued by the Authority. The aforesaid decision will be notified to the data controller upon its issuance.

5.1.2 REQUIREMENT FOR PERMIT

A permit from the Authority is required for processing data under the following circumstances:
a. automatic processing of sensitive personal data in the case where neither the data subject nor his guardian is legally able to give consent.
b. automatic processing of biometric data used for identification;
c. automatic processing of genetic data, except for processing done by doctors and specialists in a licensed medical facility and necessary for medicine and healthcare related purposes;
d. automatic processing involving the linking of personal data files of two or more data controllers handled by them for different purposes;
e. the processing, which is an optical recording, that may be used for monitoring purposes.
The Authority shall issue a decision outlining the requirements that should be complied with in order to obtain a permit to process data for any of the abovementioned forms of data processing. The Authority will contact the data controller within 30 days from receiving the permit application, and the failure to receive any response from the Authority shall constitute an implicit rejection.

6. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

Data controllers are required to notify and Authority before proceeding with data processing as well as obtaining prior permit for some forms of data processing as explained in further detail under paragraph 5 above. The Data Protection Law imposes further responsibilities and obligations on data controllers including:
• complying with the decisions of the Authority with respect to the rules and procedures of processing sensitive personal data;
• ensuring the safety of the processing by applying adequate levels of security and technical measures to avoid the unintended destruction, unauthorized access, alteration, loss of the data and protecting the data from other forms of processing;
• ensuring that the data processor is applying adequate safeguards to the data, and verifying that the data processor conducts the process in accordance with the data processing agreement entered into by the data controller and the data processor;
• maintaining confidentiality of the personal data. Data controllers are prohibited at all times from disclosing any data without the consent of the data subject or pursuant to an order of the court or public prosecutor;
• complying with the provisions of the Data Protection Law in connection with the processing of data;
• obtaining the Authority's authorization before transferring data outside the territory of Bahrain unless exempted;
• disclosing his/her identity and the intended purpose of processing the data to the data subjects;

- informing the data subjects if their data is intended to be used for direct marketing

purposes, while the data subjects shall have the right to object;

- updating the data subject with the status of any data processing application;
- receiving applications from the data subjects to correct, block, erase or withdraw their processed data; and
- keeping record of the process of processing data conducted and provide the Authority with an updated copy of the record once a month (in the absence of data protection officer).

Data controllers may be held liable in compensating a data subject who suffered damage as a result of the processing of his data.

7. DATA PROCESSOR RIGHTS AND RESPONSIBILITIES

The data processor is required to conduct the processing in accordance with the terms of the written agreement binding the data controller and the data processor, and shall only process data in accordance with the instructions of the data controller.
The same duties and obligations that are applicable to data controllers with respect to the confidentiality and security of the data are applicable to data processors.

8. DATA CONTROLLER AND PROCESSOR AGREEMENTS

How are data controller and processor relationships managed through contractual agreements and what liabilities are attached?

The law suggests that the data processor and the data controller shall be bound by a written contractual agreement. Such agreement should state that the data processor shall only conduct data processing in accordance with the instructions of the data controller, and shall bind the data processor with the same duties and obligations as the data controller with regards to data confidentiality and security.
The Data Protection Law provides that the data controller and the data protection officer shall be held liable for any damage suffered by the data subjects in connection with the processing of their information, and the data processor will not be held personally liable towards the data subjects for such compensation. We are of the view that the Data Protection Law has adopted this approach because data processors are most likely employed by the data controller and they are prohibited from conducting any processing beyond the scope of the data controller's instructions.

9. DATA SUBJECT RIGHTS

Generally, processing of personal data is prohibited without obtaining the written consent of and approval of the data subject. The Data Protection Law grants data subjects the following rights:

- to have their data stored in a manner which does make them identifiable, or having their identity encrypted if it is impossible to store their data in such manner;
- to have their data protected and not to disclose the data to any unauthorized party without the consent of the data subject;
- to be informed by the data controller when their data is being processed;
- to be informed of The data controller's full name, scope of activity or profession,

address, the purposes for which the data are intended to be processed and any other necessary information, depending on the circumstances of each case, that would ensure the fair processing for the data subject;

- to object to the use of their personal data for direct marketing or making the data publicly available;
- to object to the processing causing material or morale damage to the data subject or others;
- where data processing is used to assess the data subject's performance, financial position, extent of efficiency for borrowing, behavior or reliability, the data subject may request a different approach and not to make his/her assessment solely dependent on automatic processing of data; and
- the right to correct, block, erase or withdraw their processed data at any time by sending a written application to the data controller.

10. DATA PROTECTION OFFICER

The main duties of data protection officers revolve around the supervision of data controllers and ensuring that the data processing is being conducted in compliance with the provisions of the Data Protection Law. The Data Protection Law outlines the duties and responsibilities of data protection officers as follows:

- assisting data controllers in exercising their rights and duties in accordance with the Data Protection Law;
- acting as an intermediary between the Authority and data controllers with respect to their compliance with the provisions of the Data Protection Law and notifying the Authority with any evidenced violations or shortfalls by data controllers that have not been ratified;
- verifying the data controllers' compliance with the provisions of the Data Protection Law regarding processing data and notifying data controllers to ratify any violations thereof;
- keeping record of the data controllers' process of processing data and updating the Authority with a copy of such records once a month; and
- conducting his duties in an independent and impartial manner.

10.1. DPO – compulsory appointment (yes/no)

There is no requirement for compulsory appointment of data protection officers under the Data Protection Law. The Data Protection Law suggests that the Authority may issue a decision which requires certain categories of data controllers to appoint a data protection officer.

10.2. Requirements

Data protections officers are required to enroll in the Authority's "Register of Data Protection Officers" in order to be accredited to presume the role of data protection officers, and data protection officers are required to renew their registration annual for a fee.

The Authority shall issue a decision regulating the work of data protection officers and specifying the conditions that must be met by those who are to be registered in the said register, procedures of registration, and the period of validity and renewal thereof, as well as determining the cost of the renewal fees.

11. DATA BREACH NOTIFICATION

The Data Protection Law sets an obligation on data protection officers to notify the Authority of any violation/breach committed by the data controller, after the lapse of 10 days from the data of notifying the data controller to ratify the breach if such breach is not rectified by the data controller.

12. SANCTIONS

12.1 Civil liability

Data Protection Law suggests that anyone who suffers damages due to the processing of his data may seek compensation from the data controller or data protection officer if such processing is in breach of the provisions of the Data Protection Law.

12.2 Criminal penalties

The Data protection Law suggests that a sentence of imprisonment not exceeding one year and a fine of not less than BD 1,000 and not more than BD 20,000, or either of these penalties may be imposed on any person who commits any of the following:

- processes personal or sensitive personal data without obtaining the consent of the person subject to the data , or doing the same without notifying the Authority in advance;
- transfers data outside Bahrain without obtaining the approval of the Authority or the consent of the person subject to the data;
- provides the Authority or data subjects with false information which contradicts with the records maintained regarding processing data;
- blocks any information or data that is required to be submitted to the Authority or prevents the Authority from accessing such data;
- disrupting the work of the Authority's inspections or investigations; or
- discloses any information available to him by virtue of his work for his personal benefit.

It is to be noted that if the committer of any of the above is a corporate legal person, the fine may be increased up to twice the fine prescribed to a natural person.

Without prejudice to the penalties provided for under the Data Protection Law , the Penal Code states that "*a punishment of imprisonment for a period not exceeding one year or a fine not exceeding BD 100 shall be inflicted on a person who divulges a secret entrusted thereto in his official capacity, trade, profession or art in conditions other than those prescribed by the law or uses it for his personal benefit or for the benefit of another person, unless the person concerned with the secret allows the divulgence or use thereof*."

It is to be noted that before the enactment of the Data Protection Law, the abovementioned punishment provided under the Penal Code shall apply to any person who discloses personal data to another party for processing purposes, as we are of the view that such data qualifies as a "secret".

13. DATA RETENTION

Data subjects are entitled to request from the data controller to remove, erase or withdraw their data as mentioned under paragraph 9 above.

14. DATA TRANSFER

The Data Protection Law sets a general prohibition on transferring personal data outside the territory of Bahrain. However, there are exclusions to the general principle whereby the transfer of data outside Bahrain is allowed and they are as follows:

- The Authority shall issue a statement published in the official gazette containing a list of countries and territories to which transfer of data is permissible. The Authority will issue such list after taking into consideration territories which have applicable data protection legislation and regulations that are deemed satisfactory to the extent which ensures to the Authority the adequacy of the protection provided by the laws and regulations of the said territories.

- The Authority may authorize the transfer of data on case-by-case basis after assessing the circumstances surrounding the transfer of data. The Authority will mainly consider the size and nature of the data and purposes of the transfer thereof and the data protections laws, regulations or international conventions applicable in the territory to which data will be transferred. The authorization will be subject to the discretion of the Authority, as the Authority may set specific conditions and time periods for such authorization. ■