

Prepared by Khalifa Tours

---

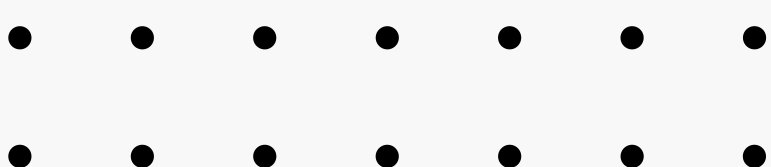
# BAHRAIN INVESTMENT COMPLIANCE SERIES 2026

Strategic Navigation of the Personal  
Data Protection Law (PDPL)

---

Verified Current as of March 2026

- +974 3166 9711
  - [www.khalifatours.co](http://www.khalifatours.co)
- 



# Personal Data Protection Law (PDPL)

Law No. (30) of 2018 | Compliance & Business Guide

## Executive Summary

The Kingdom of Bahrain's Personal Data Protection Law (PDPL) represents a pivotal shift toward international privacy standards, aligning the nation with frameworks such as the EU's GDPR. For businesses and global enterprises operating in Bahrain, compliance is no longer optional — it is a prerequisite for operational legitimacy.

This brief outlines the statutory obligations and strategic advantages of adhering to Law No. (30) of 2018 within the Bahraini business ecosystem. It is intended to be read alongside the attached full text of the Law.

## 1. Core Purpose

Under the PDPL, the legal framework serves four primary objectives:

- Data Sovereignty:** Establishing the fundamental rights of individuals (Data Subjects) to control their personal, biometric, and genetic information.
- Processing Legitimacy:** Mandating that all data processing must be anchored in a clear legal basis, such as explicit consent, contractual necessity, or legal obligation.
- Institutional Accountability:** Creating a transparent environment through the Data Protection Authority, ensuring that every data controller is identifiable and their processes auditable.
- Secure Global Interconnectivity:** Standardising the rules for cross-border data transfers to ensure that Bahraini data remains protected even when processed internationally.

## 2. Business Implications

### Compliance as a Competitive Asset

In today's regulatory landscape, 'Privacy by Design' is a value driver. Businesses establishing operations — from Family Offices to Fintech startups — in Bahrain will find that robust PDPL compliance significantly enhances institutional credibility and eases partnerships with international financial entities.

## Proactive Cost Management

Articles 33–35 may require the appointment of a Data Protection Officer (DPO) for certain sectors. This should be viewed as a fixed, foreseeable risk-management cost. Proactive implementation is far more cost-effective than facing the financial and reputational consequences of non-compliance, which can include criminal penalties of up to BHD 20,000.

## Operational Risk Mitigation

The PDPL carries meaningful enforcement provisions. Article 59 extends liability to the 'Legal Person,' meaning that in cases of gross negligence, criminal charges can extend to board members or delegated officials. Businesses are advised to conduct a top-down compliance audit as a precautionary measure — this is standard good governance practice and well within the reach of any organised entity.

*Practical note: Most liability exposure under Article 59 arises from sustained inaction rather than inadvertent errors. A documented compliance programme significantly reduces personal risk for directors and management.*

## Strategic Data Mobility

Bahrain's 'Adequacy List' — the roster of countries to which data may be lawfully transferred — is a dynamic regulatory instrument. Businesses should periodically review their cloud service providers and vendor contracts against this list to avoid disruption to international data workflows. Key jurisdictions on the list include EU member states and other GDPR-aligned nations; businesses relying on US-based cloud infrastructure should seek specific legal guidance on applicable transfer mechanisms.

---

### Legal Disclaimer

*This document is intended for informational and strategic guidance purposes only. It does not constitute legal advice. For detailed operational compliance assessments and specific legal interpretations of Law No. (30) of 2018, please consult a qualified legal practitioner licensed in the Kingdom of Bahrain, and refer to the attached full text of the Law.*

**Law No. (30) of 2018  
with Respect to Personal Data Protection Law**

**We, Hamad Bin Issa Al Khalifa,                      the King of the Kingdom of Bahrain**

- Having perused the Constitution; and
- The Civil and Commercial Procedures Law promulgated by Legislative Decree No. (12) of 1971, as amended;
- Legislative Decree No. (13) of 1972 with respect to Courts Fees, as amended;
- Law No. (13) of 1975 regulating pensions and remunerations for government employees, as amended;
- The Penal Code promulgated by Legislative Decree No. (15) of 1976, as amended;
- Legislative Decree No. (7) of 1977 with respect to Statistics and Census;
- Legislative Decree No. (9) of 1984 with respect to Central Population Register; as amended by Law No. (45) of 2006;
- Law of Evidence in Civil and Commercial matters promulgated by Legislative Decree No. (14) of 1996, as amended;
- Legislative Decree No. (28) of 2002 with Respect to Electronic Transactions, as amended;
- The Judicial Authority Law promulgated by Legislative Decree No. (42) of 2002, as amended;
- The Criminal Procedural Law promulgated by Legislative Decree No. (46) of 2002, as amended;
- Legislative Decree No. (47) of 2002 with respect to organization of Press, printing, and publishing;
- Law of Telecommunication promulgated by Legislative Decree No. (48) of 2002, as amended by Legislative Decree No (38) of 2017;
- Law No. (7) of 2003 with respect to Trade Secrets, as amended;
- Law No. (7) of 2006 ratifying Arab Charter for Human Rights;
- Law No. (46) of 2006 with respect to National Identification Card;

- Law No. (56) of 2006 with respect to Approving accession of the Government of the Kingdom of Bahrain to International Covenant on Civil and Political Rights;
- Central Bank of Bahrain and Financial Institutions Law promulgated by Law No (64) of 2006, as amended;
- Law No. (10) of 2007 with respect to Approving accession of the Government of the Kingdom of Bahrain to International Covenant on Economic, Social, and Cultural rights;
- Civil Service Law promulgated by Legislative Decree No. (48) of 2010, as amended by Legislative Decree No. (69) of 2014;
- Law No. (60) of 2014 with respect to Cybercrime.
- The Shura Council and the Council of Representatives have approved the following Law which we hereby endorse and promulgate:

#### **First Article**

Protection of personal data shall be subject to the provisions of this law.

#### **Second Article**

This Law does not derogate from rights granted by virtue of International treaties and conventions in force in the Kingdom.

#### **Third Article**

To implement provisions of this law, the Board of Directors of Personal Data Protection Authority shall issue the necessary resolutions, in a date no later than six months commencing on the first day of the month immediately following the date of its publication in the Official Gazette.

#### **Fourth Article**

The Prime Minister and the Ministers, each in his respective capacity, shall implement the provisions of this Law, which shall come into effect after one year commencing on the first day of the month immediately following the date of its publication in the Official Gazette.

**King of the Kingdom of Bahrain**  
**Hamad Bin Issa Al Khalifa**

Promulgated in Riffa Palace  
28 /10/1439 A.H.  
12/07/2018 A.D.

## Personal Data Protection Law

### Part (1) Provisions with respect to processing

#### Section One Introductory Provisions

#### Article (1) Definitions

In the course of implementing the provisions of this Law, and unless the context requires otherwise, the following words and expressions shall have the following assigned meanings:

**Data or Personal Data:** any information in any form concerning an identified individual, or an individual who can, directly or indirectly, be identified by reference, in particular, to his or her personal identification number, or by reference to one or more factors specific to his or her physical, physiological, intellectual, cultural, economic, or social identity. In determining whether an individual is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.

**Sensitive Personal Data:** any personal information revealing –directly or indirectly– about an individual’s race, ethnical origin, political or philosophical opinions, religious beliefs, affiliation to union, personal criminal record, or any information in relation to his health or sexual status.

**Processing:** any operation or set of operations which is performed upon personal data, whether or not by automatic means, including collecting, recording, organizing, classifying into groups, storing, adapting, altering, retrieving, using, disclosing by transmission, dissemination, transference or otherwise making available for others, or combining, blocking, erasing or destructing such data.

**Filing system:** any set of personal data that does not get processed by means of automatic equipment operating in response to instructions given for that purpose, but is rather structured in such a way that information relating to a particular individual's personal data is readily accessible.

**Person:** any natural or legal person, including any public entity.

**Individual:** any natural person.

**Data Controller:** a person who, either alone or jointly with other persons, determines the purposes and means of processing any particular personal data; except that where the purposes and means of the processing of personal data are determined by law, the person entrusted with the processing obligation is deemed for the purposes of this Law to be the data controller.

**Data processor:** a person, other than an employee of the data controller or data processor, who processes personal data for the Data Controller's benefit and on the Data Controller's behalf.

**Data protection guardian:** The person appointed by the Authority pursuant to Article (10) of this Law.

**Data Subject:** The person or individual subject of data.

Third party: any person other than any of the following:

1. Data subject;
2. Data controller;
3. Data processor;
4. Data protection guardian; or
5. Any person, under the direct authority of the data controller or data processor, authorized to process data for the benefit of data controller or data processor.

**Data recipient:** Any person to whom personal data is disclosed, whether a third party or not, provided that disclosure is not for the purpose of pursuing a particular jurisdiction or to exercise a particular public duty.

**Blocking:** marking stored data, by any means, to prevent its further processing, except for storing it.

**Direct marketing:** communication, by whatever means, of any marketing material or advertisement which is directed to a particular person.

**Minister:** The Minister of Justice or any other Minister designated pursuant to a Decree.

**Authority:** Personal Data Protection Authority established pursuant to Article (27) of this Law.

**Board or Board of Directors:** the Authority's Board of Directors formed pursuant to

Article (39) of this Law.

**Chairman or Board's Chairman:** The Chairman of Authority's Board of Directors.

**Chief Executive:** Chief Executive of the Authority appointed pursuant to Article (43) of this Law.

**Appeals Committee:** The committee as referred to in paragraph (2) of Article (34) of this Law.

**Investigation Committee:** The committee formed pursuant to Paragraph (5) of Article (47) of this Law.

## **Article (2)** **Scope of Application**

1. This Law shall apply to any processing, where performed as follows:

1. Processing of data by total or partial automatic means.
2. The processing by non- automatic means of data which form part of a filing system or are intended to form part of a filing system.

2. This Law shall apply to the following persons:

1. Every natural person who is habitually resident in the Kingdom or maintains a place of business in the Kingdom;
2. Every legal person with a place of business in the Kingdom;
3. Every natural or legal person not habitually resident nor maintains a place of business in the Kingdom, but processes data by using means situated in the Kingdom, unless such means are used only for purposes of transit of data over the Kingdom's territory.

3. Every legal person identified under Paragraph 2(c) of this Article shall appoint a representative who is authorized on his behalf to undertake obligations in the Kingdom as set out under this Law, and shall immediately notify the Authority about such appointment and all amendments thereof. This appointment shall not preclude any legal recourse that could otherwise be initiated by the Authority or others against the data controller upon the data controller's violation of any of his specified duties.

4. Notwithstanding provisions of Paragraph (1) of this Article, the provisions of this Law shall not apply to the following:

1. The processing of data undertaken by any individual for the sole purposes of this individual's personal or family affairs; and
2. Processing operations concerning public security handled by the Ministry of Defense, Ministry of Interior, National Guard, National Security Service, or other security body in the Kingdom.

5. The provisions of this Law shall not prejudice any duties of confidentiality in relation to the Bahrain Defense Force matters.

## Section Two General rules for legitimate Processing

### Article (3) Requirements for data quality control

The following shall be complied with, in regards to personal data that is processed:

1. Personal data is processed fairly and lawfully.
2. Personal data is collected for specific, explicit and legitimate purpose and shall not be further processed in a way incompatible with the purpose for which it was collected. Further processing of personal data for historical, statistical or scientific purposes shall not be considered incompatible with this requirement subject to ensuring that the data is not processed for supporting any decision or measure regarding a particular individual.
3. Personal data should be adequate, relevant and not excessive in relation to the purpose for which it was collected or further processed.
4. Personal data should be correct, accurate and, where relevant, kept up to date; and
5. Shall not be kept in a form which permits identification of data subject once the purpose for which the data was collected or further processed was achieved. Personal data that is stored for longer periods for historical, statistical or scientific use, shall only be kept in anonymous form, by modifying the Personal data into a form in which it cannot be associated with the data subject, if that is not possible, the identity of the data subjects must be encrypted.

### Article (4) General Conditions for legitimate Processing

Processing Personal data is prohibited without the data subject's consent, unless the processing is necessary for:

1. performance of a contract to which the data subject is a party;
2. taking steps at the request of the data subject with the purpose of entering into a contract;
3. the compliance with any legal obligation, other than an obligation imposed by contract, or the compliance with orders issued by a competent court or the Public Prosecution;
4. protecting the vital interests of the data subject; or

5. Pursuing the legitimate interests of the Data Controller or any third party to whom personal data has been disclosed to, provided that it is not in conflict with fundamental rights and freedoms of the data subject.

#### **Article (5)** **Specific Conditions for the Processing of Sensitive Personal Data**

The processing of sensitive personal data is prohibited without the data subject's consent, except where the following applies:

1. processing is necessary for the purposes of carrying out the obligations and rights of the data controller, as stipulated by law with respect to those working under his authority in the course of employment,
2. processing is necessary to protect any individual, where the data subject or the data subject's custodian, legal guardian, or conservator, is legally incapable of giving his or her consent, subject to obtaining the Authority's prior approval pursuant to Article (15) of this Law;
3. processing relates to data which is made available to the public, by the data subject;
4. processing is necessary for pursuing any legal claims or defenses, including the needed preparations thereof;
5. processing that is necessary for the purposes of preventive medicine, medical diagnosis, provision of healthcare or treatment, or for the management of healthcare services which is carried out by a licensed member of a medical profession, or by any other person who is bound by a duty of confidentiality as imposed by law;
6. processing carried out in the course of activities of associations, of all kinds, unions and other non-profit-seeking bodies, provided that:
  - a. the processing is carried out only where necessary for the purpose of what the association, union or body has been established for;
  - b. the processing relates solely to data which belongs to the members of this association, union, body or individuals who have regular contact with such association, union or body with reference to the nature of its activity; and
  - c. the data shall not to be disclosed to any other person, except where the data subject consents to such disclosure.
7. Processing is carried out by a competent public body to the extent necessary to carry out its legitimate duties as laid down by virtue of a law.
8. Processing of data relating to racial, ethnic, or religious origins where the processing is necessary for the purpose of identifying the existence or absence of equality of opportunity or treatment between members of the society of different racial or ethnic or religious origins, provided that such processing is carried out with appropriate safeguards for the rights and freedoms of data subjects as prescribed by law.

The Board shall issue a resolution setting out all rules and procedures applicable to Data Controllers with regards to the processing referred to herein.

**Article (6)**  
**Processing of data for purposes of press, literature and arts**

Articles (3), (4) and (5) of this Law shall not apply to processing of personal data carried out exclusively for purposes relating to press, arts, or literature, provided that:

1. data is correct, accurate and is kept up to date;
2. providing safeguarding measures to prevent the use of data for purposes other than those related to press, arts, and literature; and
3. processing is in compliance with laws organizing Press, printing, and publishing.

**Article (7)**  
**Processing of data with respect to instituting and pursuing of criminal proceedings, and related judgments**

1. It is prohibited to process personal data concerning instituting and pursuing of criminal proceedings, or processing of personal data in judgments reached in criminal proceedings, except for the following:

1. Processing by a competent public body if processing is necessary for the fulfillment of its legal duties;
2. Processing by any legal person, if processing is necessary for the realization of objectives that have been laid down by virtue of the law;
3. Processing by any person, as far as necessary to pursue litigations brought by or against this person.
4. Processing by attorneys at law, as far as necessary to pursue interests of their clients;
5. Processing that is necessary to carry out the profession of journalism or for scientific research purposes.

2. The exceptions granted by virtue of Paragraph (1) of this article does not derogate from the obligations of maintaining confidentiality of data as the law may prescribe. The Board shall pass a resolution setting out specific conditions and safeguards to be adhered to for protecting the confidentiality of the data referred to herein.

3. A complete register of criminal cases and judgments delivered in criminal proceedings, may be created and kept only by the Public Prosecution, Military Judiciary, Military Prosecution, Ministry of Justice, and Ministry of Interior.

**Article (8)**  
**Security of Processing**

1. The Data Controller shall implement appropriate technical and organizational measures to guarantee protection of data against accidental or unauthorized destruction, accidental loss, as well as against alteration or disclosure of, access to and any other unauthorized forms of processing. Such measures shall ensure providing appropriate level of security taking into account the latest technological security measures, the associated cost, the nature of the data to be processed and the potential risks involved. The technical and organizational measures must be recorded and accessible by all relevant parties, the Authority, Data Controller and Data Processor.
2. The Board shall pass a resolution prescribing particular conditions to be met in the technical and organizational measures referred to under Paragraph (1) of this Article. When processing personal data, the resolution may impose specific security measures on certain activities.
3. Where the data processor is entrusted with the processing of the data, the data controller shall:

1. choose a data processor who provides sufficient safeguards in respect of implementing the technical and organizational measures necessary when processing data. The data controller must take reasonable steps to ensure compliance with those measures; and
2. Ensure that the processing is only carried out pursuant to a written contract between the data processor and the data controller, which shall stipulate in particular that:
  - i. The Data Processor will only act on a processing pursuant to the data controller's instructions; and
  - ii. The Data Processor complies with obligations equivalent to those imposed on the data controller with respect to security and confidentiality.

### **Article (9)** **Confidentiality of Processing**

1. The Data Controller must not disclose any personal data without the data subject's consent or in execution of a judicial order issued by a competent court, Public Prosecution, investigation judge or Military Prosecution.
2. The Data Controller must not process any personal data in breach of the provisions of this Law. In all circumstances, an individual who has access to personal data must not undertake any processing without the data controller's consent or in execution of a judicial order issued by a competent court, investigation judge, Public Prosecution, or Military Prosecution. They also, must not use the personal data for their personal benefit, or for the benefit of others. Prohibition shall remain valid even after termination of the employment relationship or contract duration.

## **Article (10)**

### **Data Protection Guardian**

- 1.** The Data Protection Guardian is responsible for the following:
  1. Assisting the data controller in exercising his rights and adhering to his duties as prescribed under the provisions of this Law;
  2. liaising between the Authority and Data Controller with respect to the data controller's implementation of specific provisions related to the processing of personal data;
  3. ensuring that the Data Controller processes personal data in compliance with the provisions of this Law, and in the event of the Personal Data Guardian identifying any violation regarding this matter, he shall immediately bring it to the attention of the Data Controller to eliminate the causes of violation or undertake the necessary rectification as soon as possible;
  4. notifying the Authority upon obtaining new evidence concerning the committed violations which the Data Controller has not yet rectified nor eliminated its causes, after a period exceeding ten days from his notification thereof;
  5. Maintaining a register of the processing which the Data Controller is obliged to notify the Authority about, in accordance with the provisions of Article (14) of this Law. The Data Controller shall maintain the register if a Data Protection Guardian is not appointed. The register shall comprise, at least, of the information prescribed under the said Article. The Data Protection Guardian shall provide the Authority with an updated version of the register once every month ; and
  6. Data protection Guardian shall perform his duties independently and impartially.
  
- 2.** The Authority shall create a register entitled "Data Protection Guardians Register" where recognition of a Data Protection Guardian is subject to being recorded in the Register. The Board shall pass a resolution prescribing the Data Protection Guardian's duties, specifically the necessary conditions regarding who shall be recorded under the register, the procedures of recording, duration and renewal thereof.
  
- 3.** A fee shall be imposed on an application to record under the register as prescribed by Paragraph (2) of this Article. Additionally, a fee shall be imposed on an annual basis, if an application to record in the said register has been approved, and for renewals thereof. The Minister shall issue a decision, pursuant to the Council of Minister's approval, prescribing the types of fees, and identifying situations of exemptions from and refund of fee.
  
- 4.** The Data Controller may appoint a Data Protection Guardian, however, the Board may pass a resolution obliging certain categories of Data Controllers to appoint a Data Protection Guardian. In all circumstances, the Data Controller must notify the Authority within three (3) working days of such appointment.

## **Article (11) Registers Data**

1. The personal data recorded in the Registers, accessible to the public, must be within the limits of necessity, and for the purposes for which such registers were created.
2. The Board shall pass a resolution prescribing the conditions to be considered when creating the registers as referred to in Paragraph (1) of this Article.

## **Section Three Transfer of Personal Data outside the Kingdom**

### **Article (12) Transfer of personal data to countries or territories with adequate protection**

The Data Controller is prohibited from transferring personal data outside the Kingdom, except for the following cases:

1. The transfer is to a country or territory that is listed in a record compiled and updated by the Authority, comprising of countries and territories that, upon the Authority's discretion, provide adequate legislative and regulatory protection for personal data. Such record shall be published in the Official Gazette.
2. A transfer occurs upon the Authority's authorisation on a case-by-case basis provided that the data will be subject to an adequate level of protection. The adequacy of such level of protection shall be assessed in the light of all the circumstances surrounding the data transfer operation, which shall include in particular the following:
  - i. the nature of the data to be transferred, purpose and duration of processing;
  - ii. the country or territory of origin of the data, its final destination, and available measures, in such countries and territories, to protect personal data; and
  - iii. Relevant international agreements and legislations that are in force in the country or territory, which the data shall be transferred to.The aforementioned authorisation may be conditional or for a certain timeframe.

### **Article (13) Exemptions**

1. Notwithstanding the provisions of Article (12) of this Law, the Data Controller may transfer personal data outside the Kingdom to another country or territory that does not provide adequate level of protection in any of the following circumstances:

1. if the data subject has given his consent to the transfer;
2. If the transfer is for data obtained from a register compiled in accordance with the law for the purpose of providing information to the public, whether it is available for

the public or limited to any person demonstrating a legitimate interest, in accordance with certain conditions. In such case, accessing this information shall be in accordance with stipulated conditions concerning accessing the register.

3. If the transfer is necessary for:
  1. the performance of a contract between the data subject and the Data Controller or taking steps, at the request of the data subject, with the purpose of entering into a contract;
  2. the conclusion or performance of a contract entered into, in the interest of the data subject, between the Data Controller and a third party;
  3. protecting the vital interests of the data subject;
  4. Complying with an obligation prescribed in law, not being a contractual obligation, or complying with an order from a competent court, the Public Prosecution, the investigation Judge, or the Military Prosecution; or
  5. Preparing or pursuing a legal claim or defense.

2. Without prejudice to Paragraph (1) of this Article, the Authority may authorize a transfer of personal data, or collection thereof, to another country or territory that does not ensure an adequate level of protection within the meaning of Article (12) of this Law, where the Data Controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals. These safeguards may –in particular- be prescribed according to a contract to which the Data controller is a party, and the Authority shall accordingly subject the grant of such authorisation to fulfilment of certain conditions.

## Section Four Notifications and Authorizations

### Article (14) Notification to the Authority

1. The Data Controller shall give prior notice to the Authority of any wholly or partially automated processing operation, or set of such operations, intended to serve a single purpose or several related purposes.

The Data Controller is not required to give prior notice in respect of:

1. processing the sole purpose of which is the keeping, according to the law , of a register that is intended to provide information to the public and is accessible either by the public in general or limited to those with legitimate interest;
2. processing carried out in the course of activities related to associations, of all types, unions, and any non-profit-seeking body;
3. employer processing data in relation to his employees' data to the extent necessary to perform his duties, obligations, organize his matters, pursue his rights and protecting his employees' rights;
4. in situations where a Data Protection Guardian is appointed.

**2.** A resolution by the Board shall determine applicable rules and procedures to submission of the notification prescribed in Paragraph (1) of this Article, and shall specifically include the following:

1. the name and address of the Data Controller and Data Processor, if any;
2. the purpose of the processing;
3. a description of the data and categories of data subjects and the data recipients or categories of recipient;
4. any proposed transfer of data to a country or a territory outside the Kingdom; and
5. General description allowing the Authority to perform a preliminary assessment of the appropriateness of available security measures pursuant to Article (8) of this Law.

**3.** The Board may pass a resolution, where a simplified version of the notification prescribed in paragraph (1) of this Article shall be sufficient, in situations where, due to the nature of the data to be processed, no infringement to the data subject's rights and freedoms as prescribed by law shall occur. The simplified notification shall be submitted pursuant to the rules and procedures issued in the aforementioned resolution and shall include the following:

1. the purpose of the processing;
2. the processed data or categories of processed data;
3. the categories of data subjects affected by such processing and the data recipients or categories of recipient;
4. the length of time during which the data may be stored; and
5. Information required to be included within the notification.

**4.** The Authority shall within ten working days of receipt of a notification made pursuant to Paragraphs (1) or (3) of this Article, inform the Data Controller to complete any deficiency in a notification within a period not exceeding fifteen days from date of request. The applicant shall stop the processing until the notification is deemed complete.

**5.** All notifications under Paragraphs (1) and (3) of this Article shall be promptly recorded, upon its receipt, in the register referenced under Article (16) of this Law. The Authority, upon its request of the Data Controller to complete any deficiencies in a notification pursuant to Paragraph (4) of this Article, shall, by virtue of a justified resolution, write-off incomplete notification from the register. The Authority shall immediately notify the Data Controller upon the issuance of such resolution.

**6.** The Data Controller shall notify the Authority of any change with respect to the information, which the Authority was notified with pursuant to this Article, within thirty days from the date of such change.

## **Article (15)**

### **Prior Authorisation**

1. it is prohibited to process any of the following operations without obtaining the Authority's prior written authorisation:

1. Automatic processing of sensitive personal data as referenced under Paragraph (2) of Article (5) of this Law;
2. Automatic processing of biometric data necessary for the verification of an individual's identity;
3. Automatic processing of genetic data , unless carried out by physicians, or a specialist within a licensed medical establishment, and is necessary for preventative medicine, medical diagnosis or the administration of health care or treatment;
4. Automatic processing involving linkage between personal data files, of two or more data controllers, processed for different purposes; and
5. Processing that is done by means of visual recording, and used for surveillance purposes.

2. A request for authorisation shall be submitted and processed in accordance with the rules and procedures prescribed by a resolution issued by the Board. The same data should be included in the request for authorisation, and the notification prescribed in Article (14) of this Law. The Authority may, within five working days, of receipt of the request, instruct the Data Controller to complete any deficiency in the request, and the applicant shall complete such deficiency within the following five working days, or else, the Authority shall make its decision in consideration of the information given.

3. The Authority shall grant the authorisation where the request satisfies all conditions prescribed pursuant to a resolution issued by the Board. The Authority shall make a ruling on the request for authorisation and notify the concerned party of the decision within thirty days of submission thereof. If the Data Controller does not receive a reply within the period mentioned herein, it is deemed as an implied rejection.

## **Article (16)**

### **The Register**

1. The Authority shall maintain a register entitled "The Notifications and Authorisations Register" recording the following:

1. Notifications referenced under Paragraph (1) of Article (14) of this Law, and all data to be included pursuant to Paragraphs (1)(a) to (1)(d) of the same Article.
2. Notifications subject to the simplified notifications provisions in accordance with Paragraph (3) of Article (14) of this Law, and all data to be included in such notifications pursuant to Paragraphs (3)(a) to (3)(d) of the same Article.

3. What may be issued by the Authority in response to the notifications referenced under Paragraphs (1)(a) and (1)(b) of this Article.
4. Notifications that are submitted to the Authority by the Data Controllers with respect to the changes to the notification data referenced under Paragraphs (1) (a) and (1) (b) of this Article.
5. Applications for obtaining prior authorisation pursuant to the provisions of Article (15) of this Law, the data included therein and resolutions passed by the Authority with respect to prior authorisation.
6. Any other data relevant to notices and authorisation which the Authority decides to record.

**2.** The Authority shall ensure that the Register is constantly updated to reflect any changes made to this data.

**3.** Any person may, according to specially designed form, request the Authority to inspect the Notices and Authorizations Register, free of charge, during the official working hours and in the presence of a competent employee from the Authority.

**4.** Any person, according to specially designed form, and upon payment of the fee prescribed, may request from the Authority to obtain printouts from the Notices and Authorizations Register or a certificate confirming that there is no entry in the register in respect of a specified matter. The Minister shall, pursuant to the Council of Minister's approval, issue a decision prescribing the referenced fee.

## Section Five Rights of the Data Subject

### Article (17) Information to be provided to the Data Subject

**1.** In situations where data is directly obtained from the data subject, the data controller shall brief the data subject , upon registration of such data, on the following:

1. the data controller's full name, his field of activity or profession, depending on the circumstances, and his address;
2. the purposes for which the data is intended to be processed; and
3. any further information that is necessary, having regard to the specific circumstances, to ensure fair processing of data to the data subject, including the following:
  1. Names of the recipients of the data or their categories;
  2. whether replying to any of the questions addressed to the data subject is mandatory or optional, as well as the possible consequences of failure to reply;

3. the data subject's right to be notified, upon his request, of the complete data concerning him, and his right to request its rectification;
  4. whether the Personal Data will be used for direct marketing purposes; and
  5. Any further information that enables the data subject to pursue his rights as prescribed under the provisions of this Law.
2. If data was not obtained from the data subject, the Data Controller shall provide the data subject, within five days from the date of commencing registration of such data, with the following:
1. Information under Paragraph (1) of this Article;
  2. The purposes for which the data was collected; and
  3. any further information that is necessary, having regard to the specific circumstances, to ensure fair processing of data to the data subject, including the following:
    1. The information referred to under Paragraph (1)(c) of this Article;
    2. The categories of data; and
    3. The origin of the data, except where the Data Controller is legally required not to disclose this information for reasons of professional secrecy.
3. Provisions of Paragraph (2) of this Article shall not apply to the following two cases:
1. Where processing of data is undertaken for statistical purposes or for the purposes of historical or scientific research, and where notification of the data subject is not possible or involves unusually burdensome efforts. The Board by virtue of a resolution, shall determine conditions of these situations.
  2. where processing is necessary for compliance with any legal obligation, not being an obligation imposed by contract, order from a competent court, the Public Prosecution, Investigation Judge, or Military Prosecution.
4. Non- exercise of any right under Paragraph (1) of this Article or Article (20) by the Data Subject, shall not be considered as a waiver of any rights prescribed pursuant to this Section.

**Article (18)**  
**Data Subject's Request to be notified upon processing  
of his Personal Data**

1. The Data Controller, upon a request from the Data Subject with proof of identity, and free of charge, shall notify the Data Subject, within a period not exceeding 15 working days of request , if personal data concerning the Data Subject is being processed. Where such data is being processed in any way, the notification sent by the Data Controller shall be in an understandable form mentioning the following:

1. all the data being processed;
2. any information known or available to the Data Controller as to the source of the data, except where the confidentiality of the source is required by Law;
3. the purpose of the processing;
4. the names of the recipients of the data, or their categories; and
5. when such data is the sole basis for undertaking a decision that would directly affect the data subject's personal interests, the way in which the data will be used, shall be communicated in a manner that is clear to the average person, without prejudice to intellectual property rights or legitimate trade secrets.

**2.** A Data Controller, within a period not exceeding 10 days from receipt of a request made under Paragraph (1) of this Article, may notify the applicant to complete any deficiency in his request.

**3.** A data controller shall be entitled to reject incomplete requests made under Paragraph (1) of this Article, subject to complying with the requirements of Paragraph (2) of this Article and the expiry of the notification period. The Data Controller may reject a request if the Data Subject misuses his right in obtaining information. In this case, the Data Controller shall notify the applicant, within a period not exceeding fifteen working days of receipt of the request, of his reasoned decision to either accept or reject it, depending on the circumstances.

**4.** The data subject may file a complaint to the Authority against the data controller, where the request under Paragraph (1) has been rejected or if the period for response to the Data Subject's request has expired without the latter's receipt of any notice regarding the request.

### **Article (19)** **Notification to the Data Subject of the Right to Object to Direct Marketing**

Where a Data Controller anticipates that personal data which is kept by him, including personal data that is required by law to be made available to the public, may be processed for the purposes of direct marketing, the data controller shall inform the data subject of the latter's right to submit, free of charge, his objection to the Data Controller with respect to such processing,

### **Article (20)** **Right to Object to Processing for Direct Marketing Purposes**

**1.** The Data controller, within a period not exceeding 10 working days of date of receipt of a request from the data subject with proof of identity, shall not begin processing for the

purposes of direct marketing of personal data in respect of the applicant or shall cease the processing.

**2.** The Data Controller shall notify the Data Subject, free of charge, within ten working days of receipt of request with any of the following:

1. If the request has been approved
2. If the request has been partly approved, the reasons thereof and the extent of approval; or
3. Rejection of the request and reasons thereof.
4. The Data Subject may file a complaint to the Authority against the Data Controller, where the Data Subject does not accept the Data Controller's decision regarding the request, or if prescribed period has expired without the Data Subject's receipt of any notice regarding his request.

### **Article (21)**

#### **Right to object to processing causing material or moral damage to the Data Subject or Others**

**1.** The Data Controller, within a period not exceeding ten working days from date of receipt of the Data Subject's request with reasons for request, evidence thereof and proof of identity, shall not begin processing any personal data in respect of the applicant or cease the processing wholly or for a specified purpose or in a specified manner, under the following two cases:

1. the processing of that data for that purpose or in that manner is causing unwarranted substantial damage, being material or moral, to the data subject or others;
2. Where there are reasonable grounds according to which, processing for that purpose or in that manner is likely to cause unwarranted substantial damage, being material or moral, to the data subject or others

**2.** Paragraph (1) of this Article does not apply if the Data Subject consented to the processing, or when any of the situations under Article (4) paragraphs (1) to (4) of this Law apply, and in other cases as may be prescribed by a resolution issued by the Board.

**3.** Paragraph (2) of Article (20) applies to any request made pursuant to this Article.

### Article (22) Right to object to Decisions based on Automated Processing

1. If a decision is based solely on automated processing of personal data intended to assess the Data Subject regarding his performance at work, financial standing,

credit-worthiness, reliability or conduct, then the Data Subject shall have the right to request processing in a manner that is not solely automated. Reconsideration in this case shall be obligatory on the decision maker, and free of charge. The Board shall issue a resolution specifying procedures relating to submitting and processing of the request.

2. The provisions of Paragraph (1) of this Article shall not apply in favor of the Data Subject, where the decision is taken in the course of entering into or performance of a contract with the data subject, provided that suitable measures to safeguard his legitimate interests have been taken, such as hearing the Data Subject's view.

### **Article (23)**

#### **Right to request rectification, blocking and erasure of data**

1. A Data Subject may lodge a request accompanied with proof of identity to a Data Controller to rectify, block or erase the personal data relating to him when the processing of such data is in breach of the provisions of this Law, in particular if the data is inaccurate, incomplete, outdated or if its processing is illegal. The Data Controller, subject to providing a legally acceptable justification, shall respond to the request, free of charge, within a period not exceeding ten working days of receipt of the request.
2. The provision of Paragraph (1) of this Article does not apply to public registers, where the law establishing such register provides for special procedures for rectifying, blocking, or erasure of data.
3. Processing of personal data that is blocked pursuant to Paragraph (1) of this Article, is subject to obtaining consent from the data subject, or if processing is for evidentiary purposes, or for the protection of rights of a third party.
4. The provisions of Paragraph (2) of Article (20) shall apply to any request lodged pursuant to this Article.
5. Where a Data Controller has responded to a request made under Paragraph (1) – wholly or partially - he must, within fifteen days from responding to such request, notify any third party, to whom the data have been disclosed, of the rectification, erasure or blocking that was made pursuant to the request, unless this proves impossible or unachievable.

### **Article (24)**

#### **Data Subject's Consent**

1. The Data Subject's consent, in the situations referred to under this law, shall be subject to the following:

1. To be granted by a person with full legal capacity;
2. To be written, explicit, clear, and specific to the processing of certain data;
3. To be freely given by the data subject after being advised of the intended purpose or purposes of the processing, together with where the particular circumstances so require, of the consequences of refusing consent.

2. Where the Data Subject has limited or no legal capacity, the legal guardian, custodian or conservator, as prescribed by law and in accordance with the conditions under Paragraph (1)/ (b) and (c) of this Article, shall be relied on.

3. The Data Subject may at any time, give notice to the Data Controller, to withdraw his consent to the processing of his personal data. The Board shall issue a resolution prescribing the procedures for submitting such request and its determination thereof by the Data Controller.

### **Article (25)** **Lodging Complaints**

Anyone having a legitimate interest or capacity may lodge a written complaint to the Authority if he believes that there might be a breach of any provision of this Law or that a person is processing personal data in a manner inconsistent with the provisions of this Law. All complaints that may be lodged pursuant to this Law, shall be subject to a resolution issued by the Board, prescribing specific rules and procedures for lodging and processing of such complaints.

### **Article (26)** **Submission of requests, notifications, objections, complaints and exchanged of correspondences**

Pursuant to Legislative-Decree No (28) of 2002 with respect to Electronic transactions, any electronic medium, as subsequently identified by a resolution issued by the Board, may be used for submitting requests, notifications, objections, complaints and for exchanging correspondences.

## **Part II** **Data Protection Authority** **Section One: General provisions**

### **Article (27)** **Establishment of the Authority and its Logo**

1. A public authority called the “Personal Data Protection Authority” is hereby established. It shall have legal personality with financial and administrative independence and shall be subject to oversight by the Minister.
2. A Legislative-Decree shall be issued to determine the administrative body responsible for duties and powers granted to the Authority pursuant to the provisions of this Law, until the Authority’s financial provisions are allocated in the general budget of the state, and a Decree to determine formation of the Board of Directors is issued. The Decree shall identify who, in the administrative body, shall carry out the duties and powers of the Board, the Chairman, and the Chief Executive as prescribe in the provisions of this Law
3. The Board shall pass a resolution with respect to the Authority’s logo, its design and fields of use. The Authority shall have an exclusive right to use its logo and to prevent others from using it, or using an identical or similar sign to it.

### **Article (28)**

#### **Minister oversight over the Authority’s work**

1. The Authority shall submit the Minister periodic reports on the Authority’s activities and the conduct of its business. The reports shall identify in particular, what the Authority has accomplished, any impediments to the conduct of its business, if any, the underlying reasons, and measures adopted to address such impediments. The Minister may request to the Authority to provide him with any data, information, documents, minutes, records, or reports necessary to enable him to oversee Authority’s work.
2. Without prejudice to the independence enjoyed by the Authority in carrying out its duties and the exercise of its powers pursuant to the provisions of this Law, the Minister shall monitor the Authority’s compliance with both the Law and the overall policy of the state with respect to the Authority’s work, and the extent to which the Authority is competently and efficiently carrying out its duties, within its available allocated financial provisions.
3. If it became apparent to the Minister that there is any inconsistency in respect of any matter related to the conduct of business of the Authority and the provisions of the Law or the overall policy of the State, or where the Minister determines that the Authority is not realizing its objectives efficiently and competently, the Minister is entitled to object and shall notify the Authority in writing of his views with respect to such particular matter. If the Board insisted on the validity of its view, the matter shall be brought before the Council of Ministers to decide the dispute by passing a resolution within a period not exceeding thirty (30) days from the date of referral by the Minister.

### **Article (29)**

#### **Financial resources and Budget of the Authority**

1. The Authority shall have an independent budget. The beginning and end of the Authority’s financial year shall correspond to the financial year budget of the State.
2. The Authority’s financial resources shall consist of the following:

1. Allocations by the State in its general financial budget;
2. Donations and grants, in accordance with the Authority's objectives, and subject to prior approval by the Council of Ministers;
3. Amounts collected as Fees pursuant to paragraph (3) of Article (10), paragraph (4) of Article (16), and paragraph (1) of Article (34) of this Law;
4. Amounts collected as Fines pursuant to paragraph (1/b) and (1/c) of Article (55) of this Law;
5. Any other amounts collected by the Authority in the course of exercising its objective-related activities.

### **Article (30)** **Duties and powers of the Authority**

The Authority shall undertake all assigned duties and granted powers necessary to protect personal data, and it shall, in particular, carry out the following duties:

1. Informing Data Controllers and the general public on their rights and obligations pursuant to provisions of this Law;
2. Overseeing compliance with provisions of this Law;
3. Overseeing and inspecting Data Controllers' activities with respect to processing of personal data, to ensure compliance with the provisions of this Law, and to encourage developing systems that would ensure protection of such data according to this Law;
4. Receiving and reviewing of notifications pursuant to Article (14) of this Law;
5. Granting prior authorizations pursuant to Article (15) of this Law;
6. Accrediting Data Protection Guardians pursuant to Article (10) of this Law;
7. Overseeing and inspecting Data Protection Guardians' work to ensure compliance with provisions of this Law;
8. Receiving reports and complaints concerning breach of provisions of this Law, examining it, and determining its seriousness;
9. Investigating reports and complaints with respect to breach of provisions of this Law, whether submitted by others, discovered by the Authority itself, or referred to by the Minister, and deciding on the investigation pursuant to Section One of Part 3 of this Law;
10. Organizing training and educational courses and programs to raise awareness in relation to provisions of this Law, spread personal data protection culture, conducting and supporting relevant researches and studies and benefiting from its findings;
11. Studying and examining legislations relevant to personal data protection and recommending its amendments to ensure compliance with internationally accepted standards;
12. Formulating opinions about draft legislations with respect to protection of personal data;
13. Representing the Kingdom in international conferences as the competent body for protection of personal data;

14. collaborating with counterpart authorities with respect to matters of common interests;
15. Exercising other duties and powers as prescribed by this Law.

### **Article (31)**

#### **Exercising of Duties and Powers, and undertaking of Consultations**

The Authority shall carry out its duties and exercise its powers efficiently, effectively, and transparently, without discrimination and in a consistent manner, in accordance with the State's overall policy with respect to the Authority's area of work.

### **Article (32)**

#### **Conflict of Interest**

1. If the Board is considering a matter of, direct or indirect personal interest to a Board member, which conflicts with requirements of his post, such member shall notify the Board in writing of his interest as soon as he is aware of the Board's intention to consider the matter, and he may not participate in such deliberations nor vote on the matter of concern.
2. The Chief Executive and any employee of the Authority shall not have direct or indirect interest which conflicts with the requirements of their posts accordingly. Each is ought to immediately report, in writing, of any interest arising in such context during the period of holding the post at the Authority. Notifications submitted by the Authority employees' shall be addressed to the Chief Executive, and the Chief Executive's notification shall be addressed to the Board.
3. The Authority shall keep a register called (Conflict of Interests Register) where interests described in paragraph (1) and (2) of this Article shall be recorded. The Register shall state the name of the relevant person, his post or job title, details of such interest, and decisions or procedures undertaken by the Authority thereof. Access to (Conflict of Interests Register), and the right to obtain printouts or a certificate confirming that there is no entry in the register in respect of a specific matter, shall be according to provisions of paragraphs (3) and (4) of Article (16) of this Law.

### **Article (33)**

#### **Authority's Annual Reports**

1. The Authority shall prepare an annual report, to be approved by the Board, with respect to its activity and course of business in the previous financial year. The report shall highlight, in particular, the Authority's accomplished achievements, difficulties hindering its performance, if any, implemented solutions to avoid such impediments, in addition to any other suggestions which the Authority finds to be supportive of maintaining protection of personal data, or any other matter considered, by the Authority or the Minister, to be worth listing in the annual report.

2. The full Annual Report shall be published by means determined by the Board, to ensure availability of access to all, accompanied with a copy of the audited closing account concerning the same financial year, within a period not exceeding four (4) months of the end of the financial year. Subject to the Board's approval, the abstract of the annual report and the closing account, as mentioned in this Article, shall be published in the Official Gazette and in at least two local newspapers, one of which is in English and the other is in Arabic.

### **Article (34)** **Appeal against resolutions of the Authority**

1. Any decision of the Authority may be challenged by any person with an interest, and upon payment of the prescribed fee, within thirty days of becoming aware of the decision.
2. A judicial tribunal shall be established within the Authority, called (Appeal Tribunal). The Tribunal shall adjudicate appeals brought before it, pursuant to paragraph (1) of this Article. The Tribunal shall be composed according to a decision by the Minister, where members shall have a tenure of (3) years. The Tribunal shall consist of three judges of the Civil High Court of Appeal to be delegated by the Supreme Judicial Council upon the Minister's request; the longer serving of the two judges shall be President of the Tribunal. The third member of the Tribunal shall be a qualified Information Technology specialist. With the exception of judges, the Tribunal member shall take an Oath before the Minister, reading: "I swear by Almighty God to carry out my duties diligently and honestly, and to respect the laws and regulations of the Kingdom". Such member may as well participate in discussions and deliberations of appeals without voting rights in its decisions. An employee from the Authority shall act as Tribunal clerk and shall therefore attend Tribunal sessions, evidentiary procedures, taking minutes and signing it with the president of the Tribunal. The minutes and all other documents shall be kept by the clerk.
3. The Tribunal shall have the same powers vested in the Civil High Court of Appeal within its area of competence.
4. A ruling of the Tribunal shall be reasoned and adopted by the majority of its members. In case of absence of majority, where each judge adopts a different view, a third judge shall be nominated, according to paragraph (2) of this Article, to have the deciding vote. Executory formula, as provided by the clerks of the Court of Appeal, shall be attached to the Tribunal's resolution, and shall therefore be considered as a judgment delivered by the Civil High Court of Appeal. Enforcement of Tribunals resolutions and related matters thereof are within the competence of the Judge of court of Execution, in accordance with provisions of Civil and Commercial Procedural law. Tribunal's final resolution is subject to appeal before the Court of Cassation pursuant to its procedures.
5. Subject to its consistency with the nature of Tribunal's work and provisions of this Article, provisions of Civil and Commercial Procedural Law promulgated by Legislative Decree No (12) of 1971 shall apply to determine Tribunal's appeal

procedures, and mechanism of notifying persons of concern of its ruling. A Regulation issued by the Minister of Justice, after obtaining the opinion of the Authority, shall determine such details, in addition to basis for rewarding non-judicial member of the Tribunal.

6. Applicable fees to appeals brought before the Appeal Tribunal, shall be subject to the Law on Court fees with respect to cases brought before courts, to determine bases for estimation, exemptions, and deferral of fees.

### **Article (35)**

#### **Employees of the Authority**

1. Sufficient number of competent and experienced employees shall be recruited within the Authority covering its different fields of work, in addition to sufficient number of employees holding administrative and regular posts.
2. Subject to special provisions provided for in the Authority's Personnel Regulation, employees of the Authority shall be subject to provisions of Civil Service Law promulgated by Legislative Decree No (48) of 2010, and Law No (13) of 1975 regulating pensions and remunerations for government employees.

### **Article (36)**

#### **Inspection**

**1.** Inspectors, being Authority employees or others, delegated by the Chief Executive to carry out inspection duties to ensure compliance with provisions of this Law, shall be entitled to:

1. Access to premises relevant to the Authority's competence with the purpose of examination and inspection, in addition to accessing files, records, notes, documents with existing data, and having the right to obtain a copy thereof;
2. Hearing statement of any of the workers in the premises mentioned in paragraph (1/a) of this Article, who is suspected to be involved in the subject of administrative investigation.

**2.** Inspectors delegated by the Minister of Justice, by virtue of a decision issued in agreement with the Minister, are granted the capacity of Law Enforcement Officer with respect to crimes prescribed by this Law, falling within their jurisdictions, and related to their posts.

**3.** Inspectors pursuant to paragraph (1) and (2) of this Article, are prohibited from entering housing premises without prior authorization from the Public Prosecution, or investigation judge as the case maybe.

### **Article (37)**

#### **Maintaining confidentiality of information and documents**

1. The Authority, and its employees are prohibited from disclosing any information or documents submitted for the purposes of this Law without obtaining prior expressed consent from the concerned party, or his legal representative, to which such information or documents are relevant.

2. Provisions of paragraph (1) shall not apply to the following cases:

1. Information or documents, that at the time of its disclosure, was available to the public;
2. Revealing information or data in an abstract form, or as collection of information framed in a way as not to enable identification of specific person

3. Notwithstanding paragraph (1) of this Article, the Authority may disclose information and documents in any of the following circumstance:

1. Enabling any person, delegated by the Authority to carry out duties prescribed in this Law, provided that he is committed to confidentiality of received or accessible information and documents;
2. Any person of competence and experience whom the Authority need to consult, provided that he is committed to confidentiality of received or accessible information and documents;
3. When cooperating with counterpart authorities in other countries with respect to matters of common interest pursuant to paragraph (14) of Article (30) of this Law.
4. Execution of a judicial order delivered by a competent court, investigation judge, Public Prosecution, or Military Prosecution.
5. Pursuant to provisions of this Law or provisions of international treaties to which the Kingdom is a party.

### **Article (38)** **Notification to Central Bank of Bahrain (CBB)**

Chief Executive shall notify the Governor of CBB concerning any inspection which the Authority intends to carry out, pursuant to provisions of this Law, with respect to businesses of financial institutions subject to CBB monitoring. The Governor may assign any CBB employee to attend inspection and record observations.

### **Section two:** **The Board**

### **Article (39)** **Formation of the Board**

1. The Authority shall have a Board made up of seven members, including a Chairman, and shall be constituted pursuant to a Decree as follows:

1. One member nominated by the Council of Ministers;
2. One member, from the academic faculty, holding an academic rank of associate professor as a minimum requirement, with appropriate specialization with respect to the Authority's fields of business, to be nominated by University of Bahrain;
3. One member, an employee holding a senior position, to be nominated by the Telecommunications Regulatory Authority;
4. One member, an employee holding a senior position, to be nominated by the Central Bank of Bahrain;
5. One member to be nominated by Bahrain Chamber of Commerce and Industry;
6. One member to be nominated by the most representative body of stakeholders in financial institutions sector, as the Minister may determine after consultations with the Governor of Central Bank of Bahrain; and
7. One member to be nominated by the most representative body of IT specialist, as the Minister may determine

**2.** If any of the bodies referred to under Subparagraphs (e), (f), and (g) of paragraph (1) of this Article, fails to nominate candidates within (30) days of receiving notification to nominate a representative, the formation of the Board may therefore be according to the Minister's nomination for a member affiliated to the body that has failed to present its nominations within the prescribed period.

**3.** Holding the post of Minister is incompatible with holding the post of Board member;

**4.** The Decree issued with respect to formation of the Board shall specify the person holding the post of Chairman. The term of office for the Board members shall be four years renewable once for a similar term. However, with respect to the first Board, the term of office for the Chairman, and three of its members shall be four years, while the term of office for the remaining members shall be three years. The Decree issued with respect to formation of the Board shall determine term of office for each member.

**5.** The Board shall elect, from among its members, a Deputy Chairman, who shall act for the Chairman during his absence if he is unable for any reason or whenever his office falls vacant. The Deputy Chairman shall hold the post until the end of his term.

**6.** If the office of any Board member falls vacant for any reason, a replacement shall be appointed in the same manner as provided under Paragraphs (1) and (2) of this Article. The new member shall complete the term of his predecessor and if such period is less than one year, he shall be eligible for re-appointment twice.

**7.** A member of the Board may be relieved from office before the expiry of his term only pursuant to a Decree, upon recommendation made by a majority of Board members, in cases of gross failure or inability to perform his duties, or his breach of the requirements of honesty and decency

8. Remuneration of the Chairman and Board members shall be determined by a Decree.

#### **Article (40)** **Duties and Powers**

The Board is responsible for setting the Authority's policy, overseeing its work, and may take any action necessary to realize the Authority's duties and exercise its powers, and may in particular:

1. Issue regulations and resolutions, in addition to taking all measures necessary to enforce provisions of this Law;
2. Endorse the Authority's organizational structure and issue internal regulations for the affairs of its personnel matters. Such regulations shall include rules and procedures for the appointment of the Authority's staff, their promotion, transfer, wages, remuneration and disciplinary measures and other such matters, without being subject to the Civil Service Law, including rules for work ethics and values, and conditions and rules for financial disclosure of members of staff;
3. Endorse draft annual budget and audited closing account of the Authority;
4. Accept financial resources as prescribed in paragraph (2/b) of Article (29) of this Law;
5. Review the periodic reports submitted by the Chief Executive on the conduct of the Authority's business, and determining any action necessary with respect to the content of these reports;
6. The Board may assign certain duties and powers to one committee or more from among its members, to its Chairman, any of its members, or to the Chief Executive. This shall not include the power to issue regulations or resolutions within the Board's competence as prescribed under the provisions of this Law.

#### **Article (41)** **Meetings**

1. The Board shall hold an ordinary meeting at least four times each year. The Chairman may, at any time, call a special meeting of the Board. The Chairman shall also call a special meeting of the Board to be held within 15 days of the receipt of a reasoned written request addressed to him for that purpose, from either the Minister, at least two Board members, or the Chief Executive.
2. In all cases, the notice calling a meeting of the Board shall identify the purpose of the meeting and shall be accompanied with the meeting's agenda.
3. The Chief Executive may attend all meetings of the Board, except those cases prescribed in the Internal Regulations, and with no voting right during deliberations. The Board may request the attendance of any person of concern or a person with the needed expertise, for discussion or to be informed about their opinion. None of all the foregoing attendees shall have a right to vote.

4. The Board shall appoint a secretary who shall prepare its agendas, record minutes of all meetings of the Board and shall maintain all documents and records of the Board and carry out any assigned tasks, in connection with the Authority's field of work.

### **Article (42)**

#### **Quorum and Voting**

A meeting of the Board shall be duly convened if attended by a majority of its members, provided that the Chairman or the Deputy Chairman is present. Resolutions of the Board shall be made by a majority of the members present except in cases where this Law, or Regulations, or resolutions implementing its provisions, require a special majority. In the event that the votes are equally split, the vote of the Meeting chairman shall be the deciding vote.

### **Section Three:**

#### **The Chief Executive**

### **Article (43)**

#### **Appointment, remuneration, and Vacancy of Office**

1. The Authority shall have a Chief Executive who shall be appointed, pursuant to a Decree, for a three years term upon the recommendation of the Board. His term of office may not be renewed for more than two consecutive terms
2. Remuneration of the Chief Executive shall be determined by the Board, including allowances and other privileges.
3. In the event that the office of the Chief Executive falls vacant, for any reason whatsoever, a replacement shall be appointed in the same manner prescribed in paragraph (1) of this Article.
4. The Board may appoint a Deputy Chief Executive who shall act for the Chief Executive during his absence, or if he is unable for any reason, or whenever his office falls vacant. The Deputy Chief Executive shall carry out assigned duties by the Board or by the Chief Executive. The Board's resolution appointing a Deputy Chief Executive shall be published in the Official Gazette.
5. Where a Deputy Chief Executive has not been appointed pursuant to the preceding Paragraph and if the office of the Chief Executive falls vacant for any reason whatsoever, the Board shall issue a resolution that shall be published in the Official Gazette, to delegate the Chairman or any other member of the Board or any employee of the Authority, to act, temporarily, for the Chief Executive..

### **Article (44)**

#### **Duties and Powers**

1. The Chief Executive shall represent the Authority before the Courts and in its relations with third parties, and shall be accountable to the Board for the conduct of the Authority's

business, technically, administratively and financially. The Chief Executive shall assume all the powers of the Authority except for powers granted to the Board pursuant to provisions of this Law. He shall, in particular, undertake the following:

1. Manage the Authority, run its affairs, and supervise the conduct of its business and employees;
2. Implement resolutions of the Board.
3. Draw-up a proposed budget of the Authority and a report on such proposed budget and submit both to the Board , at least two months prior to the end of the financial year;
4. Draw-up a closing account of the Authority and a report on such Account, and submit both to the Board for approval, within two months from the end of the financial year;
5. Draw-up, as prescribed in Article (33) of this Law, an annual report with respect to the Authority's activity during the preceding financial year, and submit it to the Board for approval, within a period not exceeding 3 months from the end of the financial year, accompanied with a copy of the Authority's audited accounts of the same financial year.
6. Draw-up a proposed organizational structure for the Authority, and submit the same to the Board for its approval;
7. Submit to the Board periodic reports every three months, unless the Board prescribes a shorter period, on the Authority's activity, the conduct of its business and the achievements made against the set plans and programs. The reports shall identify impediments to the Authority's performance – if any- and measures proposed to address such impediments; and
8. Carry out other duties and exercise other powers that are within his competence in accordance with this Law.

2. The Chief Executive may delegate, in writing, any of the Authority's employees to carry out some of his duties to ensure that the Authority's business is adequately completed.

#### **Article (45) Resignation**

The Chief Executive may resign from office, by submitting a written request to the Board, at least three months before the specified resignation date. Acceptance of the resignation is subject to the Board's approval.

#### **Article (46) Removal from Office**

1. The Chief Executive may, pursuant to a Decree, be removed from office before the expiry of his term upon a recommendation by the majority of the Board members, but only in cases of gross failure or inability to perform his duties effectively and efficiently or his breach of the requirements of honesty and decency.
2. The Board shall enable the Chief Executive to lay his defense before recommending his removal from office, and shall record such defense in an independent record. Where the Board recommends removal from office, the Chief Executive shall continue to carry out his duties until a Decree removing him from office is issued. Nevertheless, if recommendation for removal is based on Chief Executive's violation to requirements of honesty and decency, then a resolution by the Board shall be sufficient for such effect.

### Part 3

## Accountability of Data Controller and Data Guardian

### Section One

## Accountability by the Authority

### Article (47)

## Conducting Investigation

1. The Authority may initiate an investigation on its own motion, upon receiving a request from the Minister, or based on serious reports and complaints with the purpose of investigating alleged violations to provisions of this Law by the Data controller or Data Protection Guardian. The authority may as well carry out its investigation, in presence of serious evidence suggesting that violation is imminent.
2. The Authority shall, prior to commencing investigation procedures, notify the concerned Data Controller or Data Protection Guardian as the case may be, stating the reasons behind the Authority's view that a violation has occurred or is about to occur. The notice shall identify evidence, presumptions, and information in the Authority's possession with respect to the violation. However, preliminary investigation procedures may be carried out, pursuant to the Chairman's resolution, without serving such notice, if substantial evidence lead to the belief that investigation may be hindered, or that the truth may be lost. A notice shall be served once such reasons cease to exist
3. The concerned Data Controller or Data Protection Guardian shall have the right to reply to the notice within 7 working days from receiving the notice. The reply shall contain the defense, comments, and shall be accompanied with documents, presumptions, or any other supporting evidence.
4. The Authority, upon examination of the reply to the notice, may decide to dismiss the matter, or commence investigation procedures, and in both cases, a notification shall be delivered to concerned parties.
5. The Authority may carry out the investigation, or form a tripartite internal or external committee of competent individuals. The Authority may as well assign any qualified person to carry out such task.

**Article (48)**  
**Investigation procedures**

1. The investigation committee, and upon commencement of investigation procedures, may request any party of an interest, to provide the committee within a prescribed period, with data, information, clarifications needed for investigation purposes, and relevant documents.
2. The concerned parties attending investigation sessions are entitled to be accompanied by attorneys. An attorney is allowed to speak, only when permitted by the investigation committee.
3. The investigation committee may ask the concerned parties attending the session, any question with the purpose of clarifying the matter, and may request an answer to be verbal or in writing within a prescribed period.
4. The committee shall provide the parties concerned with the investigation, a fair chance to defend their interests within the period prescribed for investigation. Accordingly, the committee shall hold hearing and discussion sessions to the parties, and their witnesses, while allowing them to state their views, and present their arguments and defenses.
5. The investigation committee shall hold necessary minutes to record its measures and proceedings.
6. If the requested data, information, clarifications, and relevant documents, by the committee, were not sufficient, or were not submitted within the prescribed period, the committee may continue its investigation and conclude findings based on the available data, information, clarifications and documents.
7. The Board may issue a resolution, stipulating additional regulations and procedures to achieve justice and fairness with respect to conducting investigation.

**Article (49)**  
**Requesting information, date, and documents from third party**

1. Without prejudice to provisions of relevant laws, the investigation committee, and upon existing of substantial evidence indicating that a third party is in possession of data, information, or documents related to the subject matter of investigation, or if it is stored in a computer program under the third party's control, the committee may therefore order the third party to submit such date, information, or documents within a prescribed period, or by allowing the committee or whoever is assigned by the committee, to access the computer program in order to reveal such date, information or documents. Non-compliance with the above, entitles the committee, through the Authority, to issue writ on a petition from the High Court, ordering the holder, to implement such order. The court may issue its order as a summary judgment without summoning the holder. The latter however may object to the court order within 8 days of its issuance, and the court may uphold, amend or quash its order. In such case, the court's decision shall be justified based on its examination of documents and after hearing holder's statement, if possible.

2. Paragraph (1) of this Article shall not apply to correspondence or papers and documents submitted by the party concerned with the investigation, to his attorney or to a consultant expert to carry out their assigned tasks.

**Article (50)**  
**Delegation of Law enforcement officers**

In carrying out its duties, the investigation committee, may delegate any of the law enforcement officers referred to in Article (36) of this Law to carry out any of their assigned duties.

**Article (51)**  
**Examination of witnesses**

Subject to provisions of Articles (65) – (68) of Law of Evidence in Civil and Commercial matters promulgated by legislative Decree No (14) of 1996, and to Article (119) of Code of criminal procedures promulgated by Legislative Decree No (46) of 2002, the investigation committee may examine any witness whom the committee deems necessary, and shall examine any witnesses upon the concerned parties' request, unless the committee finds examining witnesses, in such case, to be pointless. If the committee is of the view that the witness conduct involves a crime, it shall prepare a memorandum which the Chief Executive shall refer to the Public Prosecution.

**Article (52)**  
**Termination of investigation procedures**

The investigation Committee shall, within a period not exceeding 6 months from the date of commencement of investigation, submit to the Chief Executive, a reasoned report of its findings, accompanied with the complete investigation file. Before the expiry of the 6 months period, and upon the Committee's request, the Chief Executive may extend the prescribed period to additional period or periods not exceeding, in total, six months, provided that the delay is attributed to reasons beyond the committee's control.

**Article (53)**  
**Notification to concerned parties**

The Chief Executive shall, within 3 working days of receiving the report prescribed in Article (52) of this Law, notify the concerned parties thereof, and shall provide them with a copy of the report and its attachments. The parties concerned with the investigation are entitled to submit a memorandum with

their data, comments and supporting documents, as a defense, to the Chief Executive office within a period not exceeding 30 days from receiving the report and its attachments. In the event of investigation initiated by a complaint, and where the plaintiff exercises the right to reply to the committee's report, in such case, the plaintiff shall, and before the expiry of the specified period, provide the defendant with the a copy of his reply and supporting documents thereof via the Chief Executive Office. The defendant may, within a period equivalent to the one specified for the plaintiff, provide the Authority with his comments on the plaintiff's reply.

#### **Article (54)** **Disposition of investigation**

The report accompanied with Chief Executive Comments, shall be submitted to the Board. Submission shall be made by the Chief Executive in the first session taking place after the termination of the specified periods in paragraph (2) of Article (53) of this Law. The Board may decide to dismiss the investigation, or to declare that the alleged violation, was not proven against the Data Controller. In evidence of violation, the Board may adopt any of the measure prescribed in Article (55) of this Law, or it may refer the matter once again to the investigation committee for further inquiry, search and for completion of investigation.

#### **Article (55)** **Permitted measures in evidence of violation**

1. In evidence of violation, and without prejudice to provisions with respect to civil and criminal liability, the Board shall order the party committing the violation to, immediately or within a specified period of time, stop his conduct, and to remove reasons and effects thereof. Failure to abide by such order within the prescribed period, shall result in the Board's authority to issue the following reasoned resolutions:

1. Withdrawal of authorization granted pursuant to Article (15) of this Law, if violation is with respect to such authorization;
2. Imposing a daily penalty, to force the offender to stop his violation and remove its reasons and effects thereof. In the event of first time violation, the penalty shall not exceed BD1000/- per day. However, in the event of second time violation within 3 years from the date of issuing a decision with respect to the offender's first violation, the penalty shall be BD2000/- per day.
3. Imposing administrative penalty not exceeding twenty thousand Bahraini dinars.

**2.** In both circumstances, as prescribed in paragraph (1/b) and (1/c) of this Article, the gravity of violation, offender's intransigence, offender's benefits thereof, and damages suffered by data subject, are factors that shall be taken into consideration when estimating the penalty amount. Collection of penalty is subject to the same methods applicable to collection of amounts payable to the state, and shall have the same rank of priority granted to custom taxes payable to Public Treasury.

**5.** The Authority may, upon the Board's decision, publish a statement with respect to committed violations by Data Controller or Data protection Guardian. The Board's resolution shall determine the medium and mechanism of publishing, proportional to the gravity of the violation. Nevertheless, publishing will not take place, unless the period prescribed for submission of appeals has expired, or a final ruling with respect to committed violation is issued.

**4.** If a criminal offence was identified pursuant to the investigation, the Board shall refer the matter to the Public Prosecution.

#### **Article (56)** **Cases of Urgency**

**1.** In cases of urgency, and upon a request submitted by the party of interest, where existing evidence is suggestive of irrevocable, specific and clear violation of rights and freedoms of the party submitting the request, upon continuation of processing the data in certain manner, the Board may issue a reasoned resolution ordering the following:

1. Temporary suspension, fully or partially, of data processing;
2. Temporary blocking, fully or partially, to data

**2.** The Chief Executive shall issue a decision with respect to paragraph (1/a) and (1/b) of this Article, upon examination of documents, hearing statements of the concerned party and Data Controller, in addition to providing them with the opportunity to state their views, arguments, supporting documents, and evidence in accordance with periods and procedures specified by the Board's resolution.

**3.** The Authority or the party of interest may issue a writ on petition From the Civil High Court, to implement any resolution issued pursuant to paragraph (1) of this Article. The court may issue the order as a matter of urgency and without summoning the Data Controller. The Data Controller may object, before the court issuing the order, within 8 days from the date of issue of such order. The court may uphold, amend or quash the order thereof.

4. In the event of a resolution issued pursuant to paragraph (1) of this Article, The Chief Executive, upon discovery of any violation, shall refer the matter to investigation, subject to provisions of Section one of Part(3) of this Law.

**Section two**  
**Civil liability**

**Article (57)**  
**Compensation**

Without prejudice to provisions of the Civil Law, a party who suffers damage resulting from processing of his personal data by the Data Controller, or as a result of violating provisions of this Law by Data protection Guardian, is entitled to claim compensation from the Data Controller or Data protection Guardian as the case maybe.

**Section three**  
**Criminal Liability**

**Article (58)**  
**Penalties**

Without prejudice to any stricter penalty imposed by any other law:  
1. A person shall be liable to imprisonment for a term not exceeding one year, and / or a fine not less than BD 1000/- and not exceeding BD 20,000/- in the following circumstance:

1. processes personal data in contravention of the provisions of Articles (5);
2. transfers personal data to another country or territory in contravention of Article (12) and (13) of this Law;
3. Processes personal data without notifying the Authority in breach of paragraph (1) of Article (14) of this Law;
4. Omits to notify the authority with respect to any change to the data which was the subject of notification pursuant to paragraph (1) of Article (14) of this Law, in contravention to paragraph (6) of the same Article;
5. Processes personal data without obtaining prior authorization from the Authority, in breach of Article (15) of this Law;
6. Provides the Authority or Data subject with incorrect or misleading data, or data that is in contrary to what is recorded in registers and documents in his possession;
7. Withholds from the Authority any data, information, records, or documents to which the Authority should have access to, in order to carry out its prescribed duties by this Law;
8. Prevents or delays Authority's inspectors, or Authority's ongoing investigation;
9. Discloses data or information accessible by virtue of his post, or unlawfully uses such data and information for his personal benefit or to benefit others, in violation of the provisions of this Law;

2. A person, in breach of paragraph (1) and (2) of Article (32) of this Law, shall be liable to fine not less than BD 3,000/- and not exceeding BD 20, 000/-. In the event of conviction, a court may order confiscation of amounts resulting from the crime.

3. A person shall be liable to imprisonment for a term not exceeding one month, and / or a fine not less than BD 100/- and not exceeding BD 500/-, if he unlawfully uses the Authority's logo or if a an identical or similar sign or symbol is used.

### **Article (59)** **Liability of legal person**

Without prejudice to criminal liability of natural person, a legal person shall be subject to penalties to the lower and upper limits being double the amounts prescribed for fines, if any of the crimes stipulated in Article (58) of this Law was committed, under the legal person name, or on its behalf, or for its benefits. Provided that such crimes are the result of actions, omission, approval, cover-up, or gross negligence by any member of the Board of Directors of the legal person, or by its delegated official, or by a person acting in such capacity.

### **Article (60)** **Conciliation**

The Board, or the party delegated thereof, may agree to conciliation, except for cases of recidivism, with respect to crimes stipulated in paragraphs (1/c), (1/d), (1/e) of Article (58) of this Law; provided that the final verdict has not been issued in the relevant case, and subject to payment of minimum amount of fine within 7 days from agreement to conciliation. Criminal proceedings, concerning the criminal offense subject of conciliation, shall laps upon completion of conciliation, without prejudice to the right to claim compensation by the party suffering damage.