(For Consultation)

Draft Order

Regarding the duties of the Data Protection Guardian

After reviewing Law No. (30) of 2018 issuing the Personal Data Protection Law, and in particular Article (10)

And based on Order (xxx) regarding the fee for registering in the DPG register,

And upon the recommendation of the Chief Executive of the Authority,

Article 1

Definitions

In implementing the provisions of this Order, the following words and expressions shall have the meanings indicated opposite each of them, unless the context of the text requires otherwise:

Authority: Data Protection Authority

Law: Law No. 30 of 2018 regarding personal data protection

Register: Data Protection Guardian Register

Data Controller: Controller as defined in Article 1 of the Law

Data Protection Guardian: A person approved by the Authority whose duties are stipulated in Article (10) of the Law

Appeals Committee: The committee concerned with hearing appeals against rejected Guardian applications formed according to Order (xxx) for the year 2021

Article 2

Establishment of the register

The Authority shall establish a register in which the names of licensed Data Protection Guardians shall be listed.

Article 3

Enrollment in the register

Every natural or legal person who wishes to practice the activity of the Data Protection Guardian must enroll their names in the register.

Article 4

Eligibility for enrollment in the register

In order to be enrolled in the register to practice the activity of the Data Protection Guardian, the following requirements must be met:

First: Natural Persons

1. To be fully competent.
2. To be a holder of a Bachelor's Degree in information technology, and a professional qualification in information security, or audit on information security, or cyber security.
3. Demonstrate no less than 3 years of work experience in information technology.
4. To be of good reputation, and shall not have been finally convicted for a penalty of a breach of trust or a crime affecting his honor or integrity or if he has been convicted for a crime involving a breach of professional ethics, unless he has been reinstated.
5. Should not have been dismissed from work based on a disciplinary ruling or decision, or his license to practice his main profession had been revoked or suspended based on disciplinary ruling or decision.

Second: Legal Persons

1. Registered institution in the Kingdom of Bahrain.
2. Involved in the provision of legal, or audit, or information technology, or management consulting, or accounting, or risk management services.
3. That among its employees shall be at least three who meet the conditions established for the registration of the natural person

The registration shall be canceled if any of the aforementioned conditions are lost.

The Board of Directors of the Authority may issue a decision specifying other conditions that must be met in relation to certificates and experiences.

Article 5

Submitting the enrollment request

An application for enrollment in the register shall be submitted to the Authority via the registration form, through the channels to be announced, confirming the fulfillment of all necessary conditions in accordance with the provisions of this Order, along with the supporting documents.

Article 6

Required documents for application

The following supporting documents must be attached to the enrollment application:

- Application form (natural and legal persons)Letter of good conduct (natural persons)
- Copy of CR or license (for legal persons)
- Experience certificate (natural persons)
- Passport and/or CPR copies (natural persons, or employees with legal persons)
- Passport size photo (natural persons)
- Address and contact details (natural and legal persons)
- Qualifications and curriculum vitae (natural persons)

Article 7

Decision on application

The Authority shall issue a decision regarding the application within thirty days from the date of the application that includes all the conditions, information, and supporting documents stipulated in Article (6) of this Order, and the applicant shall be notified of it within seven days from the date of its issuance.

Failure to inform the applicant of the decision within the aforementioned periods is considered an implicit rejection of the application.

And those whose request has been rejected may appeal the Authority's decision before the Appeals Committee within seven days from the date of their knowledge of the rejection decision or the lapse of the periods specified in the first paragraph of this article.

Article 8

Enrollment fee

The applicant must pay the prescribed fee for enrollment stipulated in Order (xx) for the year 2021 regarding the prescribed fee for enrollment in the Data Protection Guardian's Register, immediately upon the approval of the enrollment request by the Authority.

Article 9

The period of enrollment and its renewal

The period of Data Protection Guardian's enrollment in the register shall be three years, starting from the date of registration.

It may be renewed for a similar period or periods with the same procedures followed for submitting the registration application and the conditions stipulated in this Order, based on an application submitted by the Data Protection Guardian within thirty days before its expiry, after paying the prescribed renewal fee.

Failure to submit the renewal application on the specified date shall result in the Data Protection Guardian's name being removed from the register.

Article 10

Termination and cancellation of enrollment

The Data Protection Guardian's enrollment expires in the following cases:

1. Death of a natural person, or a final cancellation of the enrollment for a legal person.
2. The expiry of the enrollment period unless it is renewed in accordance with the provisions of this Order.

The Data Protection Guardian's enrollment shall be revoked in the following cases:

1. Loss of any of the conditions stipulated in Article (4) of this Order.
2. It is proven that the Data Protection Guardian was enrolled based on incorrect documents or information.
3. The Data Protection Guardian requested in writing to revoke his enrollment.
4. Disciplinary penalty issued against the Data Protection Guardian by the Authority for a violation.

Article 11

Duties of the Data Protection Guardian

The Data Protection Guardian shall perform the following duties in accordance with Article 10 of the Law:

1. Ensure that the Data Controller has developed a data privacy framework covering the required technical and organizational measures, embedding requirements of the Law, and the implementing regulations.
2. Monitor the Data Controller's compliance with the requirements of the law when performing their duties and data processing activities
3. Responding to the inquiries and observations of the Authority about the processing operations and methods carried out by the Data Controller.
4. Ensure that the Data Controller reports data breaches affecting personal data to the affected data subjects and the Authority within three days of the breach occurring or becoming known.
5. Carry out an independent audit of high-risk processing operations, and ensure that the Data Controller takes the necessary measures to implement its recommendations, in order to monitor the extent of current compliance, and report on exceptions or improvements to the organization's board of directors, and ensure that they are resolved by the Data Controller.
6. Inform the competent authorities and immediately notify the Authority of violations that raise the suspicion of committing a crime punishable by law.
7. Periodic review of the effectiveness of procedures, systems, and data privacy controls established by the Data Controller.
8. Submit a report to the Authority at the end of each year, including the extent of the Data Controller's compliance with the implementation of the provisions of the law and implementing regulations, the ability to implement it and the extent of compliance with the procedures, regulations and controls related to keeping records of data processing and notification, obtaining the necessary prior authorization from the Authority, and the requests of data subjects related to the right to object to processing, rectification, blocking, and erasure. The report must also include the following:

a. The number of complaints or violations observed during the year, and the procedures that were followed to address, or resolve them and eliminate their causes.

b. Determine the need to strengthen internal control systems or develop training.

c. Any other matters decided by the Authority, which will be required by the Data Protection Guardian.

Article 12

Supervision and inspection

The Authority supervises and inspects the duties of the Data Protection Guardian to verify the extent of his compliance with the provisions of the law, and also undertakes the necessary inspections on its own initiative, or based on communications or complaints received, and takes the necessary measures regarding any violations.

Article 13

Investigations and penalties

Subject to the provisions stipulated in the first section of the third part of the law, the Authority may refer the Data Protection Guardian for investigation in the event that it is proven that they violated any of the obligations imposed under the law or the orders issued in implementation thereof.

Article 14

Disclosure

Before appointing the Data Protection Guardian, the Data Controller must complete the form prepared, for disclosure of the following information:

1. The sector or activity in which the Data Controller operates.
2. Determine whether the processing activities are fully or partially automated, and the expected volume of those processing (high, medium, low).
3. The category of data subject associated with the processing.
4. The category of data that is subject to processing (personal data or sensitive personal data).

Article 15

Appointment of the Data Protection Guardian

The Data Controller may appoint a Data Protection Guardian from the list of Data Protection Guardians enrolled in the register as stipulated in Article (2) of this Order.

The Chairman of the Board of Directors may require specific categories of Data Controllers to appoint a Data Protection Guardian, whenever he deems that the type of work, the nature of the activity, the volume of processing that takes place, or the manner of processing of personal data requires additional monitoring.

Article 16

The Chief Executive Officer of the Authority shall implement the provisions of this Order, and it shall take effect from the day following the date of its publication in the Official Gazette.