Ministry of Justice, Islamic Affairs and Waqf

Order No. (43) of 2022
Regarding the conditions to be met in the technical and organizational measures that guarantee protection of personal data

Minister of Justice, Islamic Affairs and Waqf:
After reviewing Law No. (30) of 2018 issuing the Personal Data Protection Law, in particular, Article (8) therein,

And Decree No. (78) of 2019 Determining the Administrative Entity to Assume the Duties and Powers of Personal Data Protection Authority,

And Order No. (42) of 2022 Regarding the transfer of personal data outside the Kingdom of Bahrain,

And upon the submission of the Undersecretary of Justice and Islamic Affairs,

The following has been decided upon:

Article (1)
Definitions

When implementing the provisions of this Order, the words and expressions therein shall have the meanings stipulated in the Personal Data Protection Law issued by Law No. (30) of 2018, the following words and phrases shall have the meanings set forth, unless the context requires otherwise:

Law: Personal Data Protection Law issued by Law No. (30) of 2018
Privacy by Design: A method of data processing system that seeks to proactively provide the maximum extent of privacy by ensuring that personal data is protected in a technological system or business practice by default, and applies security measures at all stages of processing in a way that anticipates and prevents privacy implications prior their occurrence.

Article (2)
Technical and organizational measures to be implemented while processing

To ensure adequate level of security, the Controller shall implement all or some of the following technical and organizational measures while processing personal data, depending on the scope, context, purposes or risks of the processing:

1- Implement the Privacy by Design program when preparing, designing, selecting and using applications, services and products that are used for processing any type of data.
2- Establishing privacy frameworks through the structure, practice, and instructions related to the protection of personal data in accordance to the Law and its Orders.
3- Implement effective measures to address breaches and its attempts aiming to mitigate its risks. For example but not limited to: (regulating and ensuring access to saved data, password protection, using anti-virus software and firewalls, complying with software licenses, regulating data retention and disposal period, regulating data backup measures, and developing appropriate technical protocols to ensure access control and security for data maintained physically and virtually).
4- Conducting a Vulnerability Assessment and Penetration Testing (VAPT) periodically to verify and measure the efficiency of the implemented security measures, and to rectify and mitigate any security vulnerabilities.
5- Develop an effective plan to address sudden breaches in data processing systems, that allows the continuation of processing without interruption.
6- Determine the competence of each concerned employee according to the task entrusted to him, to provide high protection and privacy of the processed data.

The Data Controller shall inform the concerned employees of the measures mentioned in the previous paragraph, in a manner that ensures compliance with the provisions of the Law and Orders issued according to it.

Article (3)
Data Protection Impact Assessment (DPIA)

1- The Data Controller may conduct the Data Protection Impact Assessment, taking into account the nature, scope, context and purposes of the processing, and high risks of processing on the rights and freedoms of natural persons. A single assessment may address a set of similar processing operations that present similar high risks.

2- The Data Controller shall seek the advice of the Data Protection Guardian, where designated, when carrying out a data protection impact assessment.
3- The Data Controller shall conduct the Data Protection Impact Assessment in the following cases:

a- In the cases stipulated in paragraph (1) of Article (22) of the Law, or a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b- Processing on a large scale of special categories of data or of personal data relating instituting and pursuing of criminal proceedings, and related judgements referred to Article (7) of the Law.

c- A systematic monitoring of a publicly accessible area on a large scale.

4- The assessment shall contain at least:
   a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the Data Controller;
   b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
   c. an assessment of the risks to the rights and freedoms of data subjects; and
   d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

5- Where appropriate, the Controller shall seek the views of Data Subjects or their legal representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Article (4)
Breach or violation notification

1- The Controller must establish communication channels with Data Subjects to enable them to report breaches or potential violations of personal data.

2- The Controller is obliged to document cases of breach of personal data, and to indicate their causes, effects of their occurrence, and rectification measures taken. The Controller shall establish specific procedures to inform the Authority of the occurrence of any violation or breach of data within a period not exceeding (72) hours from the date of its discovery, unless if the personal data breach would not affect the rights of Data Subjects.
If the Controller fails to notify the Authority within the aforementioned period, the notification must be accompanied by justifications for the delay.
If the Controller did not communicate the personal data breach to the Data Subject, the Authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

3- The Controller is not obliged to notify the Data Subject of the breach or violation in the following cases:

a- If the breached personal data is unintelligible to any person who is not authorised to access it, such as encryption;

b- The Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise;

c- it would involve disproportionate effort. In such a case, there shall instead be a public communication.

4- The notification of the breach or infringement incident must include the following data:

For Data Subjects:

a.Type of data breach or violation.
b. Details of the data that has been breached or violated.
c. Recommendations to mitigate effects of the breach or violation.

For the Authority:

a. Description of the nature of the personal data breach or violation including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;
b. The name and contact details of the Data Protection Guardian or other contact point where more information can be obtained from.
c. Description of the likely consequences of the personal data breach or violation.

d. Description of the measures taken or proposed to be taken by the Controller to address the personal data breach or violation, including, where appropriate, measures to mitigate its possible adverse effects.

e. Measures taken to address the main cause of the breach or violation and to prevent its recurrence.

5- Where, and in so far as, it is not possible to provide the information provided in paragraph (4) at the same time, the information may be provided in phases without undue delay.

Article (5)
Internal investigation

The Data Controller shall set clear and written rules regarding the internal investigation to reveal the reasons that led to the breach or violation of the data, and the individuals that caused the breach or violation means of receiving internal and external reports regarding the breach, and the necessity of keeping evidence related to the violation or breach and submitting it to the Authority or judicial authorities when necessary.

Article (6)
Contracting with an external processor or any third party

The Data Controller shall take into account the provisions stipulated in Article (5) of Order No. (42) of 2022 Regarding the transfer of personal data outside the Kingdom when concluding a contract with an external processor, any third party to transfer data to them.

Article (7)
Data processing by more than one Data Controller

Subject to obtaining prior authorization in accordance with article (15) of the Law, the Controller shall comply with the following, if the data is processed by more than one controller jointly:

a- Written agreement between them regarding the role and responsibilities of each to ensure compliance with the Law and its Orders.
b- Disclosing the agreement to the Data Subjects to promote transparency.
c- Determining the contact point for Data Subjects, and the communication mechanism.

Article (8)
Periodic training

The Controller shall provide periodic training programs to ensure that employees who process personal data are familiar with the Law, its orders, measures, protocols and procedures.

Article (9)
Entry into force

The Undersecretary of Justice and Islamic Affairs shall implement the provisions of this Order, and it shall come into effect on the next day following the date of publication in the Official Gazette.

Minister of Justice, Islamic Affairs and Waqf
Khalid bin Ali bin Abdulla Al Khalifa

Issued on: 14 Sha'ban 1443 AH

Corresponding to: Thursday, March 17, 2022 AD