(For Consultation)

Draft Order

Regarding the conditions to be met in the technical and organizational measures that guarantee protection of data

After reviewing Law No. (30) of 2018 issuing the Personal Data Protection Law,

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

Section One: Introductory Provisions

Article 1

The provisions of this Order shall apply to all Data Controllers who, either alone or jointly with other persons, determine the purposes and means of processing any particular personal data, by total or partial automatic means, or set of such operations, intended to serve a single purpose or several related purposes.

Article 2

The Data Controller shall implement appropriate technical and organizational measures to guarantee security of processing in accordance with the requirements of Article (8) of the Personal Data Protection Law No. (30) of 2018.

Article (3)

Organizational and technical measures shall aim at the protection of personal data as well as the processing operations and systems, In order to secure safe processing of personal data, in accordance with the law.

The Data Controller shall develop clear and specific policies and procedures to help the organization and its employees to implement their data privacy obligations.

Article (4)

The Data Controller shall adopt necessary effective measures to secure the processing systems, to mitigate privacy risks and, contribute to reducing any incidents or attempts of breach.

Article (5)

The Authority may take the necessary action to validate the technical and organizational measures adopted by the Data Controller through an inspection, audit, or investigation, as stipulated in Articles (36) and (47) in the Personal Data Protection Law No. (30) of 2018.

Section Two: Organizational and Technical Measures

Governance

Article (6)

The Data Controller shall establish a clear privacy governance structure to ensure implementation of the law and implementing regulations.

Resources and Training

Article (7)

The Data Controller may appoint an employee to carry out the duties of 'Data Protection Officer', to assist the Data Controller in accordance with Article (6) of this Order. In particular, the Data Protection Officer shall commit to the following:

a. Direct communication with data subjects, to receive inquiries, requests and complaints relating to processing of personal data;

b. Communication with the Data Protection Guardian, if necessary;

c. Maintaining necessary records in compliance with the law and implementing regulations;

d. Monitoring compliance by service providers or data processors with the provisions of the law;

e. Provision of necessary support and possible facilities when conducting an audit by the Data Protection Guardian, and during the investigation and inspection conducted by the Authority; and

f. Submission of periodic reports to the Data Controller on the progress of work assigned to him, including the work completed as well as the difficulties faced while carrying out the duties.

The Data Protection Officer shall be suitably qualified in the field of data protection. He shall also have the requisite understanding of privacy controls and risks.

Article (8)

The Data Controller shall provide the Authority with the names and contact details of the Data Protection Officer, the Information Security Officer, and the auditor or consultant referred to in Article (24) of this Order, if it is decided to appoint all or any of them in the organization.

Article (9)

The Data Controller shall provide periodic training to ensure that data processors, relevant staff, including new employees, and staff who are managerially responsible for personal data, are made aware of how to handle personal data, provided that such training includes the following:

a. Statement of obligations and responsibilities set out in the law, its implementing regulations, and any other relevant privacy and information-security laws and regulations, and the consequences of violating these laws and orders;

b. The potential consequences, both individual and corporate, of any breach of Law No. (30) of 2018, its implementing regulations, and any other relevant privacy laws and regulations;

c. The identity and responsibilities of resources from the organization-wide privacy program;

d. Methods and means of dealing with data-privacy violations, and how to report them, and when and how to report suspicious incidents to their supervisors;

e. Clarification on the organization's relevant policies and procedures; and

f. Data breach examples and trends.

The above information and guideline shall be placed in a prominent and accessible place for all employees of the organization.

Privacy Framework

Article (10)

The Data Controller shall implement a privacy program which is a structured approach to govern the processing of personal data and related activities within the organization, by ensuring compliance with the provisions of the law, protection of the rights of data subjects, provision of necessary channels to ensure direct

communication with them, and mitigation, to the extent possible, of any potential data-breach risks.

Article (11)

A 'privacy by design' framework should be considered when developing, designing, selecting and using applications, services and products that are based on processing of personal data. Data Controllers shall consider the Law and its Implementing Orders, when developing and designing such products, services and applications.

For the purpose of implementing the provisions of this Order, the concept of 'privacy by design' refers to the proactive approach that anticipates and prevents privacy issues before their occurrence, and seeks to provide maximum privacy by ensuring that personal data is protected automatically in any technological systems or business practices, and that security measures are implemented at all stages of data processing.

Article (12)

The organization shall establish Key Performance Indicators (KPIs) to monitor compliance with the data protection requirements by Data Controllers. Key performance indicators may include, but not limited to, controls such as:

a. Management framework and structure;

b. Policies and procedures related to information and cyber security, record keeping, and third-party management; and

c. Statement of the lawful basis for processing personal data in accordance with Articles (4) and (24) of the Law No. (30) of 2018 (Refer to these two articles when carrying out a processing operation and granting approval).

Article (13)

The Data Controller shall ensure that a privacy strategy is put in place, which provides guidance to the organization and reflects the nature and mission of the organization.

Article (14)

The Data Controller shall develop adequate policies and procedures relating to information security, in a manner that ensures compliance with the provisions of the Law and its Implementing Orders.

The organization's nature of business, the volume of its transactions, and methods and means of processing used shall be taken into account when developing these policies and procedures.

Article (15)

Where applicable, the Data Controller shall develop adequate procedures to enable data subjects to transfer their personal data in a commonly used electronic format from one data controller to another, conveniently and without hindrance.

Article (16)

The Data Controller shall disclose the means and purpose of processing through a privacy notice or policy that is publicly published covering:

a. Purpose of collecting data;

b. Type of data being collected; and

c. How data is used and shared with any other Controllers.

Privacy notice is disclosed on the communication channels of the organization to which the Data Controller belongs, such as corporate websites, applications and any other means through which personal data may be collected and processed.

Article (17)

Appropriate data classification and handling procedures shall be developed with the aim of providing a safe environment in which the necessary degree of protection is provided when using personal data and sensitive personal data processed across the organization, both in physical and electronic formats.

Sensitive personal data shall be classified as restricted or confidential, and more effective procedures shall be followed in this regard.

Article (18)

The Data Controller shall put in place robust and advanced technical protocols to secure access to physical locations and virtual systems where personal data is

stored. Such procedures must be communicated to all employees of the organization.

Article (19)

The Data Controller shall submit periodic reports to the organization's management on the mechanisms of implementing adequate privacy controls. Such reports shall include the following:

a. The latest developments in legislation relating to the protection of personal data, information security, and privacy;
b. Employee training;
c. Privacy resourcing and funding;
d. Violations and breaches of privacy, if any; and
e. The results of the audit on the methods and means of processing.

Information Security Officer

Article (20)

The Data Controller may appoint an 'Information Security Officer' to assume the following functions:

a. Developing information security strategies in both the short term and in the long term;

b. Designing a continuous and proactive risk-assessment program to ensure that effective controls are in place to address information security risks;

c. Overseeing all the procedures for developing and implementing the Data Controller's information security policies;

d. Implementing training, education, and awareness programs on information security; and

e. Assessing information security breaches and determining responses and ways to deal with them.

General Policies and Procedures

Article (21)

Subject to the obligations stipulated in the law, the Data Controller shall implement the following:

a. Document and maintain up to date information technology and security related policies and procedures relevant to the systems and processing operations, including but not limited to:

1. Access control and security for data maintained physically and virtually or in an electronic format.
2. Change management process.
3. Disposal of personal data in physical and electronic forms according to certain controls and requirements.
4. Password protection.
5. Device authentication.
6. Maintain audit logs.
7. Anti-virus applications.
8. Network access, including firewalls.
9. Software licensing compliance.
10. Data and hardware encryption solutions.
11. Data transfer and storage controls.
12. Data back-up measures.
13. Retention period.
14. Internal correspondence.
15. Official email.
16. Management of mobile devices, and ensuring adequacy of the protection systems used in such devices.
17. Security of wireless network (WIFI).

b. Use of dummy data when developing electronic information systems in the organization; to protect personal data from loss or damage.

Data Protection Impact Assessment (DPIA)

Article (22)

1. A Data Protection Impact Assessment (DPIA) shall be performed for any new process, product, service, program, technology, or system. Their impact on personal data will be assessed, and their potential risk on the rights of individuals will be identified according to the following controls:

a. The envisioned processing operation(s);

b. The necessity of the processing activity/activities;

c. The assessment of the risks to the rights of the data subject;

d. Identification of lawful basis for such processing;

e. Any update of consent from data subjects;

f. Update to privacy notice or policy and disclosure thereof; and

g. Notification and prior authorization requirements, as applicable, including update of the records of processing lodged with the Authority.

2. Periodic review shall be performed on the processing operations described in the DPIA, to determine whether a change in assessed risks have occurred.

Article (23)

Where appropriate, the Data Controller may consult with the data subjects and service providers concerned when performing the DPIA, to obtain insights on the intended processing activities, the protection of public interests, or the security measures of the processing activities.

Vulnerability Assessment and Penetration Testing

Article (24)

The Data Controller may perform a Vulnerability Assessment and Penetration Testing (VAPT) at least on an annual basis, to assess, and evaluate the effectiveness of the security measures implemented, in order to ascertain whether the operating systems and software are up to date, including patches and security updates, in a manner that mitigates system vulnerabilities.

The penetration is tested, and the vulnerability of the system is assessed through the assistance of an external auditor or consultant specialized in the field of information security and privacy.

The Data Controller has the responsibility to rectify any security vulnerability identified and recommended in the report submitted by the auditor or consultant, within a period not exceeding three months from the date of submitting the report. The results of the VAPT shall not be disclosed to any unauthorized party or entity.

Incident and Risk Management

Article (25)

The Data Controller shall develop appropriate incident and risk response plans to manage, contain and minimize problems arising from unexpected events, including internal and external breaches.

They shall ensure that an adequate business continuity framework is in place. Protocols and controls shall be in place to back-up personal data and ensure that it can be recovered and maintained in the event of an incident or breach.

Article (26)

1. The Data Processor, upon becoming aware of a personal data breach, shall immediately inform the Data Controller.
2. The Data Controller shall document instances of personal data breaches, causes, its effects, and the remedial action taken.
3. The Data Controller shall establish a breach notification process, to communicate to the data subject and the Authority any data breach involving personal data within 72 hours. Where the notification to the Authority is not made within the aforementioned period, it shall be accompanied by reasons for the delay.
4. The breach notification shall include at a minimum:

For Data Subjects:

a. Type of data breach;

b. Details of compromised personal data; and

c. Likely consequences of the breach on the data loss, and actions taken to recover data.

For Data Controllers:

In addition to the matters prescribed in Paragraphs (4-a) to (4-c) of this Article, the notification shall include the following:

a. Actions taken on whoever caused the incident; and

b. Actions taken to address root cause and prevent recurrence.

In cases where the Data Controller does not communicate to its data subjects regarding the breach incident, the Authority may instruct the Data Controller to do

so, if it determines that the incident poses a high risk of privacy breach to the data subjects.

Article (27)

The Data Controller shall present a valid insurance policy issued by of one of the licensed insurance companies in the Kingdom. The policy shall cover compensations resulting from violating the privacy of personal data subjects for any damage or expenses incurred by data subjects as a result of that violation, provided that the insurance coverage is (BD …. thousand). The execution of claims shall be in accordance with the legally established procedures in this regard.

Article (28)

The Data Controller shall assess high risk data processing activities and develop mitigating solutions to prevent or reduce risks. Such assessments shall be documented. Also, risks, by type or category, and the key risk indicators, shall be identified.

In addition, incidents and breaches arising from failures of information systems, performance, or processing, as well as internal and external breaches, must be recorded and remedied.

Article (29)

The Data Controller Shall review the potential data privacy risk posed by outsourcing a service or activity involving personal data processing to an external processor, including the assessment of risk of a data breach.

Transfer of Data to External Processor

Article (30)

1. Whenever data is transferred to an external processor, the following should be considered:

a. The commitment of the external processor to implement the information security controls;

b. Compliance with the information disposal controls;

c. Selection of the processor based on the criteria of competence, appropriate experience, and ability to carry out the tasks assigned to them;

d. Professional reputation; and

e. Taking into account Article (12) of the Law when transferring data to a processor outside the Kingdom.

2. Contract terms with cross-border processors shall include:

a. Specifics regarding the type of personal information to which the cross-border processor will have access at remote locations;

b. The cross-border processor's plans to protect personal information being processed;

c. Scope of responsibilities of the cross-border processor in the event of a data breach;

d. Disposal of data upon contract termination; and

e. Limitations on the use of data that ensure it will be used only for specified purposes and onward transfer or processing is prohibited, unless specified otherwise in the contract.

Article (31)

The Data Controller shall establish effective systematic internal procedures, to be approved by the organization, for verifying the identity of cross-border processors, third parties and service providers when transferring data to them. Relevant staff shall fully adhere to these procedures.

Joint Controllers

Article (32)

In the event of more than one controller being involved in the processing of personal data, an agreement between the joint controllers shall be determined which states the roles and responsibilities of each controller to achieve compliance with the Personal Data Protection Law No. (30) of 2018 and its Implementing Orders.

Audit and Investigations

Article (33)

The Data Controller shall take appropriate steps to perform ongoing privacy audits to identify and assess privacy risks, and set internal policies, procedures, and controls that ensure the protection of data subjects' rights.

The nature and extent of any privacy audit must be appropriate to the nature and size of the organization. Results of such audits must be made available upon request of the Authority.

Article (34)

The Data Controller shall develop clear rules for the investigation, in order to identify the root cause of any data breach, provided that they include procedures for reporting the incident or breach, containing the breach, evaluating the risks associated with the breach, and internal and external notifications of the breach event.

Article (35)

In the event of a data privacy incident or breach, the investigation team shall determine the nature and extent of the breach, help prevent further data loss, preserve evidence of the breach and submit such evidence to the Authority or judicial authorities, if necessary.

Article (36)

The Chief Executive of the Authority shall implement this order, and it shall be in effect on the day following its publication in the Official Gazette.