Data protection brief | **Measures required to protect data**

Kingdom of Bahrain | 28 April 2021

keypoint

Bahrain's Personal Data Protection Authority (PDPA), established under the auspices of the Ministry of Justice, Islamic Affairs and Awqaf, published three draft executive resolutions on its official website (pdp.gov.bh) on 26 April 2021 in regards to the implementation of Bahrain's personal data protection law (the PDPL). In this brief, we highlight key findings from our analysis of the draft on the technical and organisational measures required to protect data:

- Data managers are required to:
  1. Implement technical and organisational measures to ensure data is processed securely.
  2. Implement clear policies and procedures and staff must commit to data privacy.
  3. Apply measures that protect processing systems from privacy breaches and minimise hacking
  4. Put privacy governance structures in place to comply with the PDPL and related decisions.
  5. Apply a privacy programme which protects data owners' rights, sets up direct communication channels with data owners and minimises the risk of privacy violations
- The PDPA has the right to verify measures implemented by data managers through inspections, audits or investigations.
- Data managers can designate a data protection staff who must:
  1. Communicate directly with data owners - receiving data enquiries, requests and complaints
  2. Communicate with a data protection supervisor, when required
  3. Maintain registers as set out in the law
  4. Monitor compliance of service providers and data processors with the PDPL
  5. Support and facilitate audits (data protection supervisor) and investigations or inspections (by the PDPA)
  6. Report to the data manager on duties accomplished and challenges faced
- Data protection staff must be adequately qualified in terms of data protection and be familiar with controls and privacy risks.
- Data managers are required to provide the PDPA with the names and contact information of data protection and information security staff when appointed.
- Data managers are required to provide frequent training programmes to ensure that data processors, staff members (including new recruits) and management understand how to handle personal data, including:
  1. The data manager's PDPL obligations, PDPL-related decisions, other laws and regulations related to privacy and information security, and the consequences of violating these laws and decisions.
  2. The legal implications (on the person or entity) of violating the PDPL and other privacy-related laws.
  3. The roles and responsibilities of resources handling privacy programmes
  4. How to handle privacy breaches and how to report them to supervisors
  5. Data privacy policies and procedures
  6. Examples of data privacy violations
- "Privacy by design" should be considered when preparing, designing, selecting and utilising applications, services and products which process data.

keypoint

- Organisations are required to implement key performance indicators to monitor compliance with data protection requirements, including:
  1. Organisational structure and framework
  2. Policies and procedures related to information security, record keeping and management of external parties
  3. Legal basis for processing personal data
- Data managers are required to set information security policies and procedures which ensure PDPL compliance. These policies and procedures should consider the nature of the organisation's business, transaction volumes and methods of processing.
- Using a published privacy policy (which should be posted on the organisation's communication channels, website and apps), data managers are required to declare:
  1. Purposes of processing data
  2. Types of data collected
  3. Methods of processing data and sharing with other data managers
- Data managers are required to implement procedures which allow data owners to port their electronic data (according to common standard) from one data manager to another without any obstacles.
- Data managers are required to implement enhanced technical protocols – which must be communicated to all staff - to ensure access to the locations and systems where data is stored.
- Data managers are required to implement procedures to classify data to create a secure environment which adequately protects physical and electronic data. Sensitive personal data must be classified as "restricted" or "confidential" with stricter protections.

Information security

- Data managers may wish to appoint an information security employee to:
  1. Develop short- and long-term information security strategies
  2. Prepare ongoing, preventative programmes to evaluate risks, applying effective measures to deal with information security risks
  3. Supervise, develop and implement information security policies and procedures
  4. Deploy information security training and awareness programmes
  5. Evaluate information security breaches and define mitigation actions.
- Data managers are obliged to:
  1. Use dummy data when developing IT systems to protect personal data from loss or destruction
  2. Document and frequently update information security policies and procedures, which include:
     - Access to physical/electronic data
     - Process for update management
     - Disposal of personal data (physical and electronic)
     - Password protection
     - Verification of devices
     - Audit reports
     - Antivirus
     - Access to networks, include firewalls
     - Compliance with software licensing
     - Encryption of devices and data
     - Data transfer and storage controls
     - Backup procedure
     - Data retention period
     - Internal communications
     - Verified emails
     - Management and security of mobile and portable devices
     - Wi-fi networks

Your success is our business

keypoint

Data protection impact assessments

- The impact on data protection must be assessed for any processing operation, product, service, technology or new system. Data privacy controls (in terms of personal data and potential risks to individual rights) must assess:
  1. Required processing operation
  2. Importance of processing operations
  3. Risks which may impact data owners' rights
  4. Legal basis for processing
  5. Conditions under which renewal of consent is required
  6. Updates to privacy policies
  7. Prior notices and approvals from the PDPA

Vulnerability assessment and penetration testing (VAPT)

- Data managers are required to annually evaluate implemented security measures and their effectiveness and verify that operating systems and software are updated and patched to close vulnerabilities.
- Data managers must remedy any security vulnerabilities within three months of being reported by an auditor or consultant.
- VAPT tests should not be disclosed to any third-party.

Incident and risk management

- Data managers are required to set appropriate plans to combat incidents and risks cause by sudden incidents, including internal and external violations.
- Data managers are required to ensure a business continuity framework is available and that protocols and controls are in place to back up and restore data in case of a breach or hack.
- Data managers are required to document and report data privacy incidents or breaches to data owners and the PDPA within 72 hours of discovery.
- Data managers are required to present a valid insurance certificate (issued by a licensed company in Bahrain) which covers compensations to data owners affected by data privacy incidents and costs incurred due to such incidents.

Transfers of data to outsourced processors

- Contract signed with outsourced processors (outside Bahrain) must include:
  1. Details of the types of data that will be available for the overseas processor
  2. Outsourcing provider's plan to protect personal data
  3. The outsourced processor's responsibilities in case of a data breach
  4. How data will be dealt with after any contract period ends
  5. Controls and restrictions on data processing, and prohibition of data transfer to other parties or processing in ways other than the ones specified in the contract
- Where data is processed by more than one data manager, an agreement must be in place to define the roles and responsibilities of each data manager.

Contact us:

Srikant Ranganathan
Senior director | IT consulting
srikant.ranganathan@keypoint.com
+973 1720 6827

Ajit Kushwaha
Lead | Data protection
ajit.kushwaha@keypoint.com
+973 1710 3494

Omar Rayan
Senior consultant | IT consulting
omar.rayan@keypoint.com
+973 1710 3497