Bahrain's personal data protection law (PDPL)

keypoint

Bahrain issued Law 30 of 2018 - the personal data protection law (PDPL) - on 19 July 2018, with the law coming into effect from 1 August 2019. The PDPL applies to any entity processing personal data wholly or partly by automated means – as well as the manual processing of personal data as part of an organised filing system.

The PDPL require a range of changes to the way businesses process personal data in Bahrain. Entities are required to seek prior approval from the relevant data protection authorities (DPAs) when collecting, processing and storing personal data. The PDPL imposes new obligations on how businesses manage data, including ensuring that personal data is processed fairly, that data owners are notified when their personal data is collected and processed, that collected personal data is stored securely, and that data owners can exercise their rights directly with businesses. The PDPL consists of 60 articles divided into three chapters:

- Chapter 1: Processing provisions: Definitions and general rules for processing, data processing and transfer controls, and the rights of data holders
- Chapter 2: Data protection authority: Establishment of the regulator, and its rights and responsibilities
- Chapter 3: Accountability of the data manager (data controller) and data processor: Accountability to the regulator, investigation procedures, civil and criminal liability, and penalties for violations

The PDPL enforces a range of criminal and administrative fines:

- Criminal offences include the processing of sensitive personal data, the transfer of personal data outside Bahrain, and the failure to notify as required - fines of up to BD20,000 or imprisonment for up to one year
- Administrative fines - up to BD20,000 (one-off fines) or daily penalties of up to BD1,000 (may increase for repeat offences)

Who is affected?

The PDPL applies to residents (including workers) in Bahrain, local businesses and businesses outside Bahrain that process personal data "by means available within the Kingdom" other than for purely transitory purposes.

What data needs to be protected?

Personal data: Any information of any form relating to an identified or identifiable individual, either directly or indirectly, particularly through personal ID numbers or physical, physiological, intellectual, cultural or economic characteristics or social identity.

Sensitive personal data: Any personal information that reveals – even indirectly – an individual's race, ethnicity, political or philosophical views, religious beliefs, union affiliation or criminal record – and any data related to health or sexual activities.

How will the law be enforced?

Bahrain will have a new data protection authority, the Personal Data Protection Authority (PDPA). The PDPA will enforce the law and have the power to investigate violations of the PDPL on its own, at the request of the responsible minister, or in response to a complaint.

Your success is our priority

What should organisations do now?

To comply with the PDPL, organisations must:

- Determine what personal data they acquire and process
- Show they meet the requirements for processing personal data
- Apply measures to protect data against unintentional or unauthorised destruction, accidental loss, unauthorised alteration, disclosure or access, or any other form of processing
- Show how they ensure confidentiality when processing data
- Appoint data protection supervisors to liaise with, or report to, the DPA as and when required

Why Keypoint?

Keypoint's data privacy team has significant experience in data privacy and protection assessments, having been engaged on a number of projects related to data classification, end-to-end data process reviews and data life cycles. We have also been engaged by clients to implement various information security-related controls.

Our 4 As approach

1. Assess

When assessing the impact of PDPL, we consider:

- The type of data held and processed
- The source of that data
- The location of that data
- The security of that data
- What is done with the data
- Why the data is needed
- Whether it is shared or transferred to third parties

2. Analyse

- Review policies and procedures
- Discover data and assess the impact
- Assess the data governance process
- Review data sharing with third parties
- Assess training and user awareness requirements
- Review data flows and data mapping
- Ascertain data security level implemented

3. Advise

- Define data flow diagrams and data classification
- Define architecture for operational functions
- Define data mapping
- Define security controls for data protection
- Define access level controls
- Define end-to-end security to store, process and transmit data

4. Assist

- Create data protection policies
- Create data flow and classification diagrams
- Create technical documents
- Train staff
- Conduct regular reviews

Contact us

Srikant Ranganathan
Senior Director
srikant.ranganathan@keypoint.com
T +973 1720 6827