

Solution spotlight | Bahrain's personal data protection law

Kingdom of Bahrain | 08 December 2022



Bahrain's personal data protection law (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 fundamentally changes the way businesses process personal data in Bahrain.

Entities are required to seek prior approval from the relevant data protection authority (DPA) 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
- Data owners are notified when their personal data is collected and processed
- Personal data, once collected, is stored securely
- Data owners can exercise their rights directly with businesses

Who is affected by the PDPL?

The PDPL applies to local businesses and residents in Bahrain, as well as businesses outside Bahrain that process personal data "by means available within the kingdom" other than for purely transitory purposes.

What kind of 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.

What should Bahrain businesses do now?

To comply with the PDPL, organisations must:

- Determine what personal data they acquire and process
- Be able to show they meet processing requirements for 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
- Be able to show how they ensure confidentiality when processing data
- Be ready to appoint data protection supervisors to liaise with, or report to, the DPA as and when required

Why Keypoint?

Keypoint's data team has significant data privacy and protection experience, having been engaged on data classification projects, end-to-end data process reviews and data life cycles. We have also been engaged to implement information security-related controls. Our data protection services include:

- Data protection assessments and audits
- Implementation of data protection systems
- Outsourcing of data protection officers

Contact us:



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



Prakash D'mello
Senior Consultant | IT consulting
prakash.dmello@keypoint.com
+973 1720 6806