



Data Protection: As a way of life

July 2018

kpmg.com/bh





The European Union (EU)'s General Data Protection Regulation (GDPR) had organizations of all sizes busy getting their houses in order in a bid to achieve compliance by the implementation date. Recently, the Kingdom of Bahrain issued a Personal Data Protection Law, due to be implemented by all organizations across the Kingdom by 1 August 2019.

Both the Data Protection Laws affect organizations that deal with consumers and businesses in EU member states and Bahrain respectively, aiming to transform the way that personal information is collected, stored, used, disclosed and disposed of.

While meeting regulatory obligations is a must, organizations should not treat the Laws as a one-off, 'tick the box' compliance activity, rather it should initiate a deliberate move towards a more privacy-conscious culture - where transparency, citizens' rights and accountability become second nature to all employees.










Organizations located outside the EU

In addition to the local Data Privacy Protection Law, organizations should be aware of the requirements of GDPR as any company dealing with data from EU data subjects needs to comply with the GDPR. The globalization of business means that many organizations are likely to handle such data in some form — even if it relates to just ONE customer or employee. The GDPR impacts collection, use and disclosure of data for organizations outside of the EU, which is likely to have considerable impact on a global level.

With many of today's international organizations typically involved in a complex web of subsidiaries and outsourced providers, the onus is on your data controller to ensure that every part of the value chain applies the same high standards of privacy protection. GDPR is not just about customers, employees in the EU also fall under the new regulation. Any financial, health and other sensitive, personal information needs to be handled in a way that meets the new standards.

Similarities: Bahrain's Data Protection Law and GDPR

The local Personal Data Protection Law and GDPR are very similar in the requirements, although there are some variations in the specifics of executing the requirements, as the theme of both the Laws are the same. Listed below are some key requirements that are similar in both the Laws.

Requirement	Bahrain	EU
 1. Scope of application	Applies to all data of physical or legal citizens in Bahrain, in whole or in part, processed using automated and non-automated means within the Kingdom	Applies to all data of EU citizens, in whole or in part, processed using automated and non-automated means within or outside EU
 2. Supervisory authority	A Personal Data Protection Authority to be established with powers and duties to implement the provision of the Law	Independent public authorities to be established by each EU member state to monitor application of the Regulation
 3. Certification	Mandatory for the Data Protection Supervisor to be accredited by the Authority	Voluntary certification to be sought by the person (natural or legal) who process data from certification bodies established by member states
 4. Data protection officer	Data Protection Supervisor, accredited by the Authority, ensures compliance with the provisions of Law	Data Protection Officer ensures compliance with the provisions of the Regulation
 5. Rights of data subjects	Rights include right to rectification, blocking and erasure of their personal data	Rights include right to rectification, erasure and restriction of processing their personal data
 6. Consent	Explicit consent to be sought from data subject prior to processing their data	
 7. Processing of sensitive data	Prior written permission to be sought from the Authority for processing sensitive personal data	Processing of sensitive data is prohibited unless it is for one of the provisions listed in Article 9 of the Regulation
 8. Fines	Violation of provisions of the Law may attract a penalty of BD1,000-20,000 and/or imprisonment for up to one year	A tiered fining structure depending on infringement. Level 1 is 2 percent of global turnover or €10 million (whichever is higher). Level 2 is 4% of global turnover or €20 million (whichever is higher).
 9. Implementation date	1 August 2019	25 May 2018

Privacy protection as a culture

Compliance deadlines inevitably focus the corporate mind. In the case of data protection, any attempts to meet regulatory obligations should not be at the expense of a longer-term strategy that acknowledges data protection, as a source of competitive advantage. By considering how your organization can meet the needs of customers and employees, you can build a privacy-aware culture and governance infrastructure which puts the right information at everyone's fingertips and consistently demonstrates transparency.

Key questions for boards

- Who is in charge of privacy protection compliance?
- Are the right accountability and governance structures in place?
- Are we prepared to speak publicly and to our customers about how we manage their data?
- How do I know whether employees are taking an ethical stance towards privacy protection?
- Do we have a data strategy? Is it focused on what is best for the customer?
- Are we handling our key customer touch points efficiently and appropriately?
- What actions are we taking to nurture a privacy-aware culture to earn and retain our customers trust?
- Do we view the data protection as a one-off initiative? Or is it part of a proactive risk management approach, enabling us to put our customers at the center of everything we do?



Quick data protection checklist

- | | |
|--|---|
| <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Do you have insight about which (sensitive) personal data your organisation processes, and what kind of impact the (inter)national and sector-specific laws and regulations have on your customer and HR data? <input checked="" type="checkbox"/> Have you assigned ownership, roles and responsibility in data protection in a clear manner? <input checked="" type="checkbox"/> Is there an internal privacy protection policy available, compliant with regulations, which describes how the organisation tends to address the privacy protection principles and who is accountable? <input checked="" type="checkbox"/> Are there procedures describing retention periods for personal data? <input checked="" type="checkbox"/> Is privacy addressed in a contractual and operational way in the event of outsourcing of IT services? <input checked="" type="checkbox"/> Are exchanges of large amounts of customer and personnel data with third parties performed in a compliant and secure manner and is there a data processing agreement in place? <input checked="" type="checkbox"/> Have you assessed cyber security and security certifications (e.g. ISO27001/2), both from client and involved third parties? <input checked="" type="checkbox"/> Have you assessed the maturity of internal controls where personal data is being processed? | <ul style="list-style-type: none"> <input checked="" type="checkbox"/> To what extent are you familiar with existing and future laws and regulations in the area of privacy protection? <input checked="" type="checkbox"/> To what extent is access to personal data limited? To what extent are adequate security measures in place to protect personal data? <input checked="" type="checkbox"/> To what extent are you able to handle customer requests on their own data, such as seeing, correcting, supplementing or deleting personal data? <input checked="" type="checkbox"/> To what extent are you familiar with the obligation to report data leaks and have procedures in place in case a data breach occurs? <input checked="" type="checkbox"/> Is privacy protection compliance periodically tested/audited, monitored and reported? Do you have adequate information to reduce privacy-related risks? <input checked="" type="checkbox"/> Are staff trained on data protection and the corresponding 'hard and soft' controls? <input checked="" type="checkbox"/> How is the maturity of the IT department? Can you rely on the IT general controls (ITGC)? <input checked="" type="checkbox"/> Have privacy incidents (data leakages) occurred and have these been reported to the authorities? |
|--|---|

Our services

Our privacy service has been designed on the basis that organizations need tailored risk-based solutions to address their individual privacy needs, risk appetite and future business strategy. Its modular and layered structure enables targeted and tailored solutions to be designed, developed, implemented and monitored consistently, guiding you through the complexity of privacy and complex global organizations.

1. Define

Articulate the strategic links between business goals, risks and personal information processing activities, and set high-level financial and resource needs for privacy management across your organization.

2. Assess

Undertake assessments to identify legal, technical and managerial risks associated with privacy compliance and areas where the organizations may be misinterpreting privacy requirements, or failing to leverage the value of personal information.

3. Design

With an understanding of the current state and applicable privacy requirements and priorities, help your organization design the right approach to addressing privacy compliance.

4. Implement

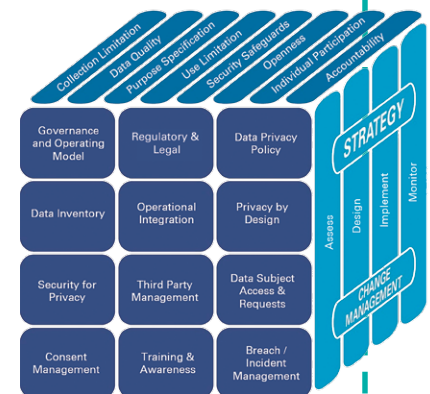
Establish legal and corporate policies, objectives, and implement pragmatic privacy structures and controls to manage privacy risks in the context of your organization's overall business risks. Our modular and layered structure enables targeted and tailored solutions to be developed and delivered at any level – from individual process to entire global organization.

5. Monitor

Help your organization design, implement and maintain a privacy monitoring framework, enabling timely assessment of governance structures and controls, and adherence to processes and procedures.

Privacy management framework

Our framework elements are the distinct elements that organizations employ to manage privacy. They provide a practical and pragmatic structure for organizing the day-to-day management and oversight required to manage privacy.



We can perform a concurrent review of the organization's compliance with the local Data Protection Law as well as GDPR.

Please do not hesitate to get in contact to find out how we can help you to prepare for the new Bahraini Personal Data Protection Law and the European GDPR regime:



Jeyapriya Partiban
Partner, Risk Consulting
KPMG in Bahrain
T: +973 17222322
M: +973 39603823
jeyapriyapartiban@kpmg.com



Ramesh Gajula
Director, Risk Consulting
KPMG in Bahrain
T: +973 17222377
M: +973 39067635
rgajula@kpmg.com



Weldon Marquis
Associate Director, Risk Consulting
KPMG in Bahrain
T: +973 17222350
M: +973 33067875
wmarquis@kpmg.com

kpmg.com/bh



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

©2018 KPMG Fakhro, a Bahrain partnership registered with the Ministry of Industry, Commerce and Tourism (MOICT), Kingdom of Bahrain and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.