Data privacy & regulations

2018 I Kingdom of Bahrain

Background

Organisations in the Middle East dealing with European data need to comply with the European Union's General Data Protection Regulations. The GDPR have been in effect since April 2016 and came into force for businesses on 25 May 2018. The regulations mandate data breach notifications and stronger privacy protections for consumers, as well as stringent data security requirements. They also provide privacy regulators with stronger enforcement powers. To comply with the GDPR, GCC-based organisations dealing with European data need to:

1. Demonstrate the ability to manage and protect EU residents' data
2. Demonstrate the ability to report breaches within 72 hours to the data protection authorities or the data subjects themselves
3. Appoint data protection officers or representatives to liaise with, or report to, the DPA as and when required

The GDPR impact business' legal and compliance, technology and data-related operations.

Complying with the regulations may require organisations to:

1. Educate stakeholders through awareness sessions
2. Assess impact and readiness
3. Identify data subject data held by organisations
4. Establish or revisit data governance processes
5. Revisit legal and compliance processes to incorporate additions to consent processes
6. Reassess technology areas to address 'privacy by design'

Our GDPR impact assessment approach

Keypoint's data privacy professionals have performed a number of GDPR and other data-related impact assessments. When assessing the impact of GDPR, we consider:

Our GDPR impact assessment approach

Keypoint's data privacy professionals have performed a number of GDPR and other data-related impact assessments. When assessing the impact of GDPR, we consider:

1. The type of data held and processed
2. The source of that data
3. The location of that data
4. The security of that data
5. What is done with the data
6. Why the data is needed
7. Whether it is shared or transferred to third parties

We adopt a three-phase approach:

1. Analyse

An onsite data audit working with the business to:

1. Review policies and procedures
2. Discover data and assess impact
3. Assess data governance
4. Review third party procedures
5. Assess training and user awareness requirements
6. Assess 'privacy by design' for technology in use
7. Assess websites and mobile apps

2. Report

Report findings through a risk and action plan, highlighting gaps and issues.

3. Execute

Support the development and implementation of updates procedures and systems.

Work products

1. Impact assessment report
2. Compliance roadmap

Where business happens

Bahrain publishes data protection law

In July, Bahrain issued Law 30 of 2018, the personal data protection law (PDPL). The PDPL comes into force on 1 August 2019, giving businesses limited time to prepare for the new regime.

The PDPL gives individuals in Bahrain rights in relation to how their personal data can be collected, processed and stored. It imposes new obligations on how businesses manage data, including ensuring that personal data is processed fairly, that data owners are notified of when their personal data is collected and processed, that personal data they collect is stored securely, and that data owners can exercise their rights directly with businesses.

The PDPL includes a new authority to investigate allegations of violations of the law. The authority can issue orders to stop violations. Compensation for individuals who incur damage as a result of their personal data being violated is included in the law, as well as criminal penalties for violations of certain provisions.

Businesses in Bahrain should pay close attention to new obligations in the PDPL – and also be aware that the PDPL differs in certain aspects from the European Union's GDPR (covered in a previous edition of this newsletter).

Our GDPR team

Srikant Ranganathan
Director
+973 1720 6827

Srikant Ranganathan is a director at Keypoint. He has advised clients in the Middle East, North Africa and India on the optimal use of IT for over 25 years.

Prior to joining Keypoint, he was a senior executive with a range of 'Big 4' professional services firms in the GCC and India, as well as running his own successful business.

Srikant is a certified information systems security professional (CISSP), a certified information systems auditor (CISA), a certified fraud examiner (CFE) and a chartered accountant (ACA).

Srikant has a deep understanding of data privacy and security requirements and has advised organisations on how to secure confidential information. He has advised on clients on how to set up, monitor and manage information security programmes in line with international standards and benchmarks.

Nishith Saxena
Executive Manager
+973 1720 6822

Nishith Saxena leads the digital transformation and enterprise systems practice for Keypoint. He has advised clients on business transformation projects for over 15 years. Prior to joining Keypoint, he was a senior executive with Big 4 firms in South Africa and India.

Nishith is a certified project management professional and is an active member of technical forums in the GCC and South Africa. He has developed a range of thought leadership on data privacy and emerging technology.

Nishith has led data privacy assessments, as well as data transformation and migration projects. He has advised a range of clients on digital transformation and customer experience enhancement projects.

He has been contributing to GDPR forums for the last twelve months and has led successful seminars and closed room senior management awareness sessions for leading organisations across the GCC.