Data Privacy Frameworks in MENA

Emerging approaches and common principles

EXECUTIVE SUMMARY

June 2019

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

To download the full report, please visit gsma.at/privacy-mena

Follow the GSMA on Twitter: @GSMA

For more information on this paper, contact Ammar Hamadien, Head of Strategic Engagement, Government and Regulatory Affairs - MENA, at ahamadien@gsma.com

Established in the UAE for 40 years, PwC has more than 5,200 people in 12 countries across the region: Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Oman, the Palestinian territories, Qatar, Saudi Arabia and the United Arab Emirates. We partner with our region's governments and businesses, to help solve the region's most important problems and build trust in our society. We are investing in the very best talent, providing an unparalleled range of expert capabilities from Legal, through Advisory and Consulting to Tax, Strategy, Digital Trust and Assurance Services, underpinned by the standout digital platform in the region.

Published June 2019

Executive summary

Importance of privacy and data protection frameworks

The increase in global data privacy regulations and both public and media awareness of data sharing and ownership are creating new challenges and opportunities that impact consumers and businesses globally.

In today's world, the value of data as a strategic asset and powerful source of economic value is clear.[1] New business models are built on data and data science and analytics. To protect consumers' privacy, and to support their own new data-driven business models, businesses need to appropriately manage and secure their data. New regulatory requirements confirm this importance, whether for personal or non-personal data. The misuse or mismanagement of data can strongly influence the public perception of an organisation in the market. Conversely, an organisation can also gain competitive advantage and customer trust through 'data protection by design' and 'by default' principles, privacy-enhancing technologies and accountability measures. These are some of the many benefits of putting appropriate privacy frameworks in place.

One of the other benefits is that implementing consistent, principles-based, risk-based, horizontal privacy frameworks at the national level can create the right conditions for data sharing across a region, leading to regional economic growth, and harmonised privacy protections for consumers.

1. For more information on the complex nature of data value chains, refer to the GSMA report, "The Data Value Chain", available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/06/GSMA_Data_Value_Chain_June_2018.pdf.

Current status of data protection in MENA

Generally, the position in most of the Middle East North Africa (**MENA**) jurisdictions is that the privacy of an individual and the safeguarding of their personal data are provided under general provisions of law rather than laws specifically focused on the issue of "data privacy" or "data protection". There are, of course, some exceptions to this, as indicated in the report.

With the General Data Protection Regulation (**GDPR**), the EU is leading the charge on data privacy and protection, and the feeling in the MENA region is that it would be a positive move for nations to introduce specific, local data protection laws to follow the GDPR. A Middle East-wide data protection model law or framework would be considered to benefit both the countries and consumers at large; however, the opportunity for regional interoperability is not being leveraged at present.

Across the Gulf Cooperation Council (**GCC**) countries, jurisdictions like Bahrain and the UAE Free Zones of the DIFC and ADGM are leading the way, with robust data protection laws on the statute books. These laws are all heavily influenced by EU 1995 Data Protection Directive (**1995 Directive**), each enshrining the globally accepted fundamental principles of data protection. It therefore follows that these jurisdictions present significant opportunities for interoperability subject to the principles of lawful use, purpose limitation, data security and data minimisation. Through interoperability, those jurisdictions with mirroring data protection regimes can work together through, for example, negotiated codes of conduct that would encompass common protections together with any additional necessary, mutually agreed elements.

Saudi Arabia and the UAE are expected to soon follow Bahrain and the Free Zones. However, it is not clear whether such laws will be sector-specific or will cover all organisations, both public and private, or indeed when such laws will be put in place. Most recently, the UAE passed the Federal Law No 2 of 2019 which regulates the use of information technology and communications in the healthcare sector. This law seeks to raise the minimum bar for protection of health data and introduces certain concepts that are on a par with best international practice in data privacy law.

Additionally, while there are regulators covering other digital issues, specific data protection authorities have not been put in place, which has created some issues around enforcement of data protection laws and awareness of the implication and interpretation of those laws. However, across those countries with specific data protection laws, there has been some momentum towards the establishment of designated, independent data protection supervisory authorities. For example, the Saudi Arabian Commission for Cybersecurity (**SACC**) recently issued a public tender to include the set up of the SACC as the regulator for personal data protection and freedom of information.

As this report indicates, where privacy laws do exist, the principles and requirements underpinning those laws reflect those enshrined in the GDPR and its predecessor, the 1995 Directive. In some cases, those same principles are reflected in other types of laws and frameworks across the region, such as cybercrime laws. As the GSMA noted in the report *Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation*,[2] identifying commonalities and differences between privacy frameworks is a first step in building a common regional approach to privacy protection and accountable data flows.

2. GSMA report, available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

Moving towards interoperability in MENA

The GDPR has spurred the creation and revision of privacy laws around the world, including in the MENA region. While many of these new and updated regimes draw heavily from their European counterparts, the possibility for divergence remains a risk, which can occur for a number of reasons including cultural and socio-political nuances across the different jurisdictions. Similar divergences occurred in Europe with the 1995 Directive, such as divergences in data localisation rules, registration and enforcement, and led to the birth of the GDPR which is directly applicable and almost completely harmonised across all 27 Member States.

Such divergences can often translate into differing levels of regulatory stringency which can lead to operational complications and significant cost burdens for organisations processing personal data of citizens in multiple jurisdictions. Similarly, grappling with strict data localisation requirements or other hard barriers to cross-border data transfers are likely to have a negative economic impact.

The benefit of a harmonised, sub-regional data protection framework for MENA is that it would encourage greater convergence across the region and bridge data protection gaps, enabling less restricted data flows while maintaining a similar level of data protection and reducing inconsistencies.

In addition, unified regional frameworks can:

- reduce barriers to investment that restrictive data flow rules can cause;
- foster greater regional economic integration and cooperation;
- create a clearer compliance environment for businesses in which to operate; and
- help guide local-level regulations which can assist countries in better integrating with their regional neighbours.

There are of course certain barriers to achieving a regional privacy framework, particularly in terms of feasibility given the different status of data privacy laws (or lack thereof) across the region. The cost of implementation, the time needed to negotiate and achieve this, and the availability of the requisite skills and expertise required to manage the process must equally be considered. A regional framework must continually evolve in order to address these challenges.

In terms of how a regional framework may be achieved, a bi- or multilateral agreement based on the principle of interoperability can allow data protection authorities and other relevant government stakeholders to share knowledge, perspective, best practices, and to consider how to improve and harmonise the national data protection frameworks. Rules regarding equivalence mechanisms or adequacy of protection can also encourage countries in the region to recognise similar levels of data protection offered by other countries' national laws.

European privacy law is designed to protect individuals' data and to ensure the free flow of protected, secure data across the EU as well as to other countries with equivalent privacy protections. The proliferation of EU-inspired data protection laws also, in many cases, reflects the balance between the expectation of privacy and the need for commercial growth and innovation. This balance should be considered in national laws, and in the context of any regional frameworks. The key message to the MENA region is that there is a significant move towards a world where laws and regulations will regulate the ways in which organisations can responsibly use personal data. These laws should reflect the dual governmental objectives of protecting citizens while also enabling growth and innovation, leading to a range of benefits for citizens and businesses alike.

Scope of this report

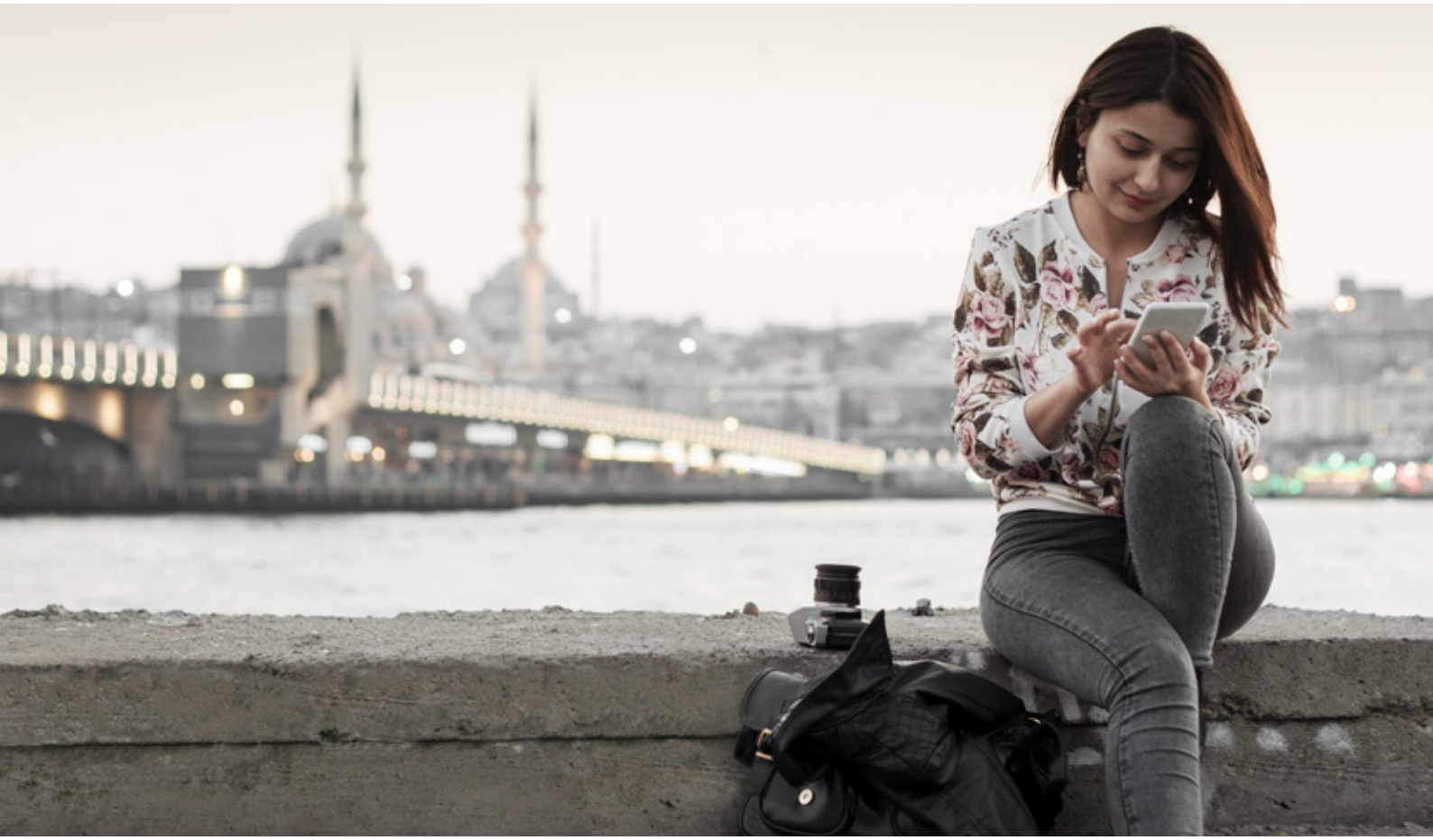
The purpose of this report is to provide an understanding of the data privacy and protection laws and regulations that currently exist in thirteen jurisdictions in the MENA region: the United Arab Emirates, the UAE Free Zones of the DIFC and ADGM, Saudi Arabia, Jordan, Kuwait, Egypt, Oman, Bahrain, Lebanon, Qatar, the Qatar Financial Centre and Turkey.

In those jurisdictions with no specific data privacy and protection legislation, the report instead considers those laws containing requirements around personal data protection and most relevant to the telecommunications sector, namely telecommunications laws and cybersecurity laws.

The report also considers these laws as they relate to other leading data privacy and protection regimes globally, specifically the GDPR. The mapping exercise focussed on the following core aspects of the GDPR:

- Cross-border data transfers;
- Data subject rights;
- Data security requirements;
- Principles of data processing;
- Data controller and data processor obligations;
- Administrative fines and regulatory sanctions; and
- Role and powers of any relevant data protection authorities.

While written on behalf of the GSMA, the perspective is wide and may cover several industry sectors.



Jurisdictional overview

JURISDICTION	OVERVIEW
BAHRAIN	Bahrain was one of the first of the GCC nations to adopt its own data privacy law in 2018 which will come into force on 1 August 2019. The law aims to be consistent with international best practices and is heavily based on the GDPR. It includes the protection of individuals' privacy and specific consent requirements for data Processing, as well as the creation of a Personal Data Protection Authority. The law is directly influenced by the country's ambitious plans to become a hub for data centres.
EGYPT	Like many other MENA jurisdictions, Egypt does not currently have a specific data protection law. A draft law regulating the freedom of data exchange and data protection is currently under discussion but has not been published. A final version of the draft is expected in 2019. The new law purports to establish a Centre for Personal Data Protection that will make and formulate various policies and regulations, and will be tasked with monitoring compliance with, and enforcing the provisions of, the new law.
JORDAN	There is currently no specific data protection law in Jordan however, a draft data protection bill is currently under consultation. The draft bill appears broadly based on the GDPR, with the incorporation of the main concepts of transparency, accuracy, storage limitation and data minimisation. However, the 2018 draft is generally accepted to suffer from issues around a lack of independence of the Jordanian Privacy Commission, a failure to incorporate international standards and best practices for data protection and insufficient consideration for modern forms of data processing.
KUWAIT	There is currently no specific data protection law in Kuwait. There are limited provisions in cyber security and electronic transactions legislation however the jurisdiction lags behind other GCC nations. However, with the focus on cybersecurity, and the efforts of the Communication and Information Technology Regulatory Authority to improve the standards and practices of information security, and protect the IT infrastructure in Kuwait, it is expected that there will be developments in data protection in the near future.
LEBANON	Data protection is governed in Lebanon by the E-Transactions and Personal Data Law, introduced in 2004 and updated in 2018. The framework has been criticised for being weak and somewhat outdated by not reflecting the reality of online data and that the substantive provisions include vague and open-ended requirements. Additionally, experts say that the law fails to adequately protect Lebanese citizens' and residents' data by putting in place weak safeguards and only granting authority to the executive branch of the Lebanese Government. Compared with the GDPR, the law is not as detailed or comprehensive, primarily as it fails to provide for the establishment of an independent regulatory body in charge of monitoring ersonal Data protection.

GDPR ALIGNMENT KEY

Aligned with the GDPR **Partially aligned with the GDPR** **Not aligned with the GDPR**

JURISDICTION	OVERVIEW
OMAN	Oman does not currently have a specific privacy or data protection law, but the Oman Information Technology Authority announced in 2017 that it was developing a data protection law. There is, however, no clear indication of when it will be published. It was reported that if approved and signed into law, the law will grant powerful rights to individuals in Oman, enabling them to exercise GDPR-style levels of control over their Personal Data including the ability to object to the Processing of their Personal Data and demand access to any Personal Data about them held by any organisation in Oman.
QATAR	Qatar was the first GCC nation to issue a generally applicable data protection law which took effect in 2017 and executive regulations further implementing it are expected to be passed in 2019. The law is modelled on and incorporates familiar concepts from other international privacy frameworks, such as the 1995 Directive (and by extension the GDPR) and mandates that any party who Processes Personal Data adhere to the principles of transparency, fairness and respect for human dignity. The Ministry of Transport and Communications is responsible for implementing and enforcing the law.
QATAR FINANCIAL CENTRE	The QFC introduced its own Data Protection Regulations in 2005 and established a Data Protection Directorate responsible for implementing and enforcing the law, managing related disputes and applying GDPR standards. The regulations are largely modelled on, and inspired by, the privacy and data protection principles and guidelines contained in the 1995 Directive and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
SAUDI ARABIA	While Saudi Arabia doesn't have a specific data protection law, media reports suggest that a new freedom of information and protection of private data law is currently under review. A novel and innovative regulatory framework for cloud computing exists; one of only a few examples of cloud-specific regulatory frameworks around the world. The framework is based on the best international practice and public consultation.
TURKEY	Turkey's Data Protection Law is predominantly modelled on the 1995 Directive, with many of the terms and central provisions very closely mirroring their equivalents in the EU law. Enactment of the Data Protection Law marks a new era for data protection in Turkey. Although the Data Protection Law is still in its infancy and no enforcement actions have yet been taken, the Personal Data Protection Board (the national supervisory authority in Turkey) has published the draft versions of secondary legislation, as well as booklets providing guidance on the implementation of the law.
UAE	The UAE does not have a specific federal data protection law analogous to the GDPR. However, reports suggest that a draft federal law (or laws) are in the pipeline although there is no indication of when such may be published. Telecommunications and Cyber Crime laws provide some limited data protection rights and obligations in the UAE alongside the Constitution and Penal Code. Telecoms service providers have certain Personal Data protection obligations under the Consumer Protection Regulations.
UAE FREE ZONES	Each of the DIFC and ADGM have enacted their own data protection laws based on international best practice, which apply to organisations in their jurisdiction. The DIFC and ADGM laws are generally consistent with data protection laws in other developed jurisdictions (specifically the 1995 Directive and the UK Data Protection Act 1998). Both have deliberately sought not to pre-empt the GDPR – rather they have adopted a "wait and see" approach before further aligning themselves with it.

GDPR ALIGNMENT KEY

Aligned with the GDPR **Partially aligned with the GDPR** **Not aligned with the GDPR**

To download the full report, please visit
gsma.at/privacy-mena

GSMA DUBAI
7 Floor ESO-24-T3
Sheikh Rashid Tower
World Trade Centre
P.O. Box 9204
Dubai, United Arab Emirates
Tel: +971 4 3097022