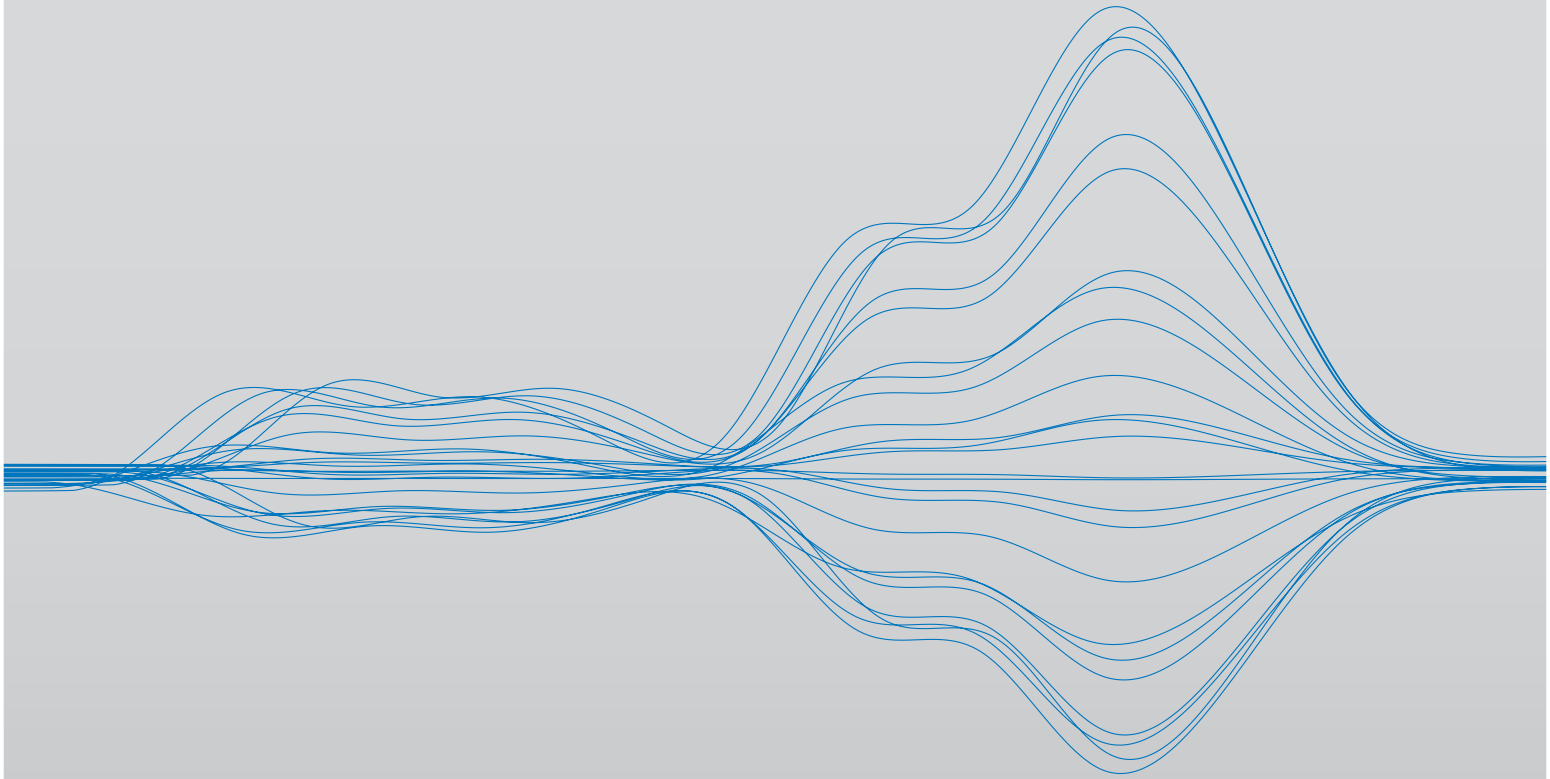
DATA PROTECTION GROUP

Practical Global Privacy



Data protection in the Middle East:
managing the regulatory patchwork

DLA PIPER

Data protection in the Middle East: managing the regulatory patchwork

The economies of the Middle East, and particularly those countries constituting the Gulf Cooperation Council (GCC) consisting of Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates, are dominated by countries looking to transition away from dependence on oil and petrochemicals. That's why many of the GCC countries, like Saudi Arabia and the United Arab Emirates, have established ambitions to become world leaders in digitisation and digital technology.

But that can't be done without the necessary national infrastructure, which includes robust data protection laws.

As these countries embrace the digital economy, they are now establishing legal frameworks to harness the potential of digitisation while at the same time protect individuals' data. But due to a lack of centralised policy at the intra-national level, and some degree of competition between the countries, they're doing so at different speeds, and with different degrees of certainty and clarity.

So how is data protection regulation developing in the Middle East? What challenges are there for global organizations, and how should they address them?

Legislation developing at a varying pace

The Middle East is a diverse region, with countries vying for international inward investment and seeking to create environments enabling digitisation and digital entrepreneurialism. As mentioned above, there is not, as yet, an overarching policy regarding data protection in the GCC (by contrast to the European Union). For these reasons, data protection regulation in the Middle East region isn't developing in a uniform manner, or at a uniform rate. The upshot is a disparate set data protection laws and regulations across the region.

The genesis of data protection laws in the region also started at different times for different reasons. For example, the first comprehensive data protection law (as is commonly understood, for example, in the form of the EU's GDPR) was one issued in 2007 by the Dubai International Financial Centre (DIFC) free zone. The driver for this early adoption is thought to have been to support the development of the DIFC as a world class financial hub that would attract entities keen to show their commitment to working within the bounds of a good regulatory framework.

Other sector regulators have also been keen to show that they are promoting good practices in data protection. As such, there have also been early sector led regulations issued by regulators seeking to manage how entities in those sectors dealt with customer information, but which often focus on elements of data protection, but which would not be considered comprehensive data protection laws.

However, in 2016 Qatar issued the GCC's first national data protection law. Since then we have seen most of the other countries in the GCC adopt comprehensive data protection laws which apply at a national level (often containing exceptions that allow for existing data protection regulations to remain in place, or which exempt some types of data, for example, data of government entities).

More recently again, some regional jurisdictions have established or amended their data protection frameworks by broadly mirror the European Union's GDPR, albeit that some regional laws introduce local adaptations. Examples include the DIFC and Abu Dhabi Global Market (ADGM), which updated their data protection laws in 2020 and 2021 respectively to more closely align with the GDPR.

However, this disparate approach has led to certain complexities to be considered by data controllers working across the region, including around lawful bases of processing or allowing data transfers. For example, with respect to data transfers outside of a country, some countries or sectoral regulators have introduced either a requirement for locally collected data to remain within the country; or complex processes for transferring such abroad. Examples of this exist in Saudi Arabia especially.

At the same time, the actual enforcement of data protection rules can be said to be light touch in some countries, for a number of reasons:

- Recent legislation might still be in its grace period for adoption, or only just out of it.
- There is sometimes no official guidance on enforcement practice.
- There can be a lack of clarity in the guidance that has been issued.
- Some countries have no national data protection regulator – the UAE being an example, which at the date of writing does not yet have a functioning regulator overseeing its national data protection law.
- Certain regulators remain focused on educating organizations about how to comply with the country's data protection legislation, rather than seeking to enforce the laws immediately.

A complex picture in UAE and Saudi Arabia

Let's take a closer look the particular challenges for organizations in complying with data protection law in the UAE and Saudi Arabia.

UAE

Although the UAE now has a federally applicable personal data protection law the picture in the UAE is complicated by the existence of multiple sets of rules across the nation's seven Emirates, including in some of its free zones, as well as certain sectoral regulatory frameworks, in health, finance and telecoms.

A federal personal data protection law (UAE PDPL) was published towards the end of 2021. But at the time of writing, no implementation guidelines have been issued, and the country has no national data protection regulator to clarify matters.

To complicate things further, two emirates have established financial free zones: the Dubai International Financial Centre (DIFC) and Abu Dhabi Global Market (ADGM). Both of these financial free zones have their own rigorous data protection frameworks – now both aligned with the GDPR – and each has an active regulator in place. There is also a health free zone in Dubai emirate, the Dubai Health Care City (DHCC), which has rules regarding the treatment of patient data.

As noted above, there are also specific rules for handling data in some sectors, outside of each of these free zones – such as in healthcare and finance at the federal and emirate level.

For this reason, businesses entering the UAE will need to be aware of where they are established (for example, the DIFC, ADGM or the DHCC, or "onshore", or even if they are acting from abroad), what fields their services could be described as falling into (in case they might be regulated by a sectoral regulator for example, medical devices that collect personal data and transmit this to a cloud service may be regulated by health regulators but also telecoms regulators to the extent that they will need to be type approved for connectivity), and where their customers, or customers' clients might be. These, and other factors, will determine which laws and regulations the business needs to comply with.

SAUDI ARABIA

The Saudi Arabian data protection framework has been undergoing changes over several years. There is currently a set of interim regulations (so called Personal Data Protection Interim Regulations, or PDPIR), which are overseen by a regulator called the National Data Management Office (NDMO). Without any real fanfare, the NDMO introduced the PDPIR as part of the National Data Governance Interim Regulations in June 2020.

The regulations govern important issues such as the protection of personal data, and the rules for transferring Saudi data abroad. Yet their legal status is unclear. The PDPIR were not published in the Saudi Arabian Official Gazette, the NDMO made no official announcement when issuing them, and there are penalties for non-compliance.

The rules on personal data transfer under the PDPIR on cross-border transfers are onerous. They require firms to gain approval from the firm's relevant industry regulator, which must coordinate with the NDMO.

In September 2021, the Saudi Government issued a personal data protection law (KSA PDPL). The KSA PDPL was slated to come into effect in March 2022. However, the KSA PDPL was considered to be very restrictive, in particular around the rules for transfer of personal data outside of KSA, the breach of which could result in imprisonment or criminal fines.

Just prior to the KSA PDPL becoming effective in March 2022, its effective date was announced to be postponed for one year. We believe this was because of, amongst other things, the onerous restrictions on data transfer and the corresponding criminal penalties.

And again, just prior to the publication of this article, the Saudi Arabian government has published a set of proposed amendments to the KSA PDPL, which, if passed, will relax a number of constraints in the proposed KSA PDPL, including:

- Introducing a concept of processing of personal data based upon "lawful interest" which appears similar to "legitimate interest" under the GDPR.
- Allowing for transfers of personal data to countries that the regulator will identify as having appropriate protections.
- Removing the criminal penalty for breach of the data transfer rules, (although there are still criminal penalties for disclosing sensitive personal data if the violation is committed with the intention of causing damage to the data subject or achieving a personal benefit).

Adopt the gold standard

Given these complexities, taking a common approach to data compliance across the Middle East will prove challenging.

There is a lack of data regarding the legal status and actual enforcement of some of these laws. Some of these laws, for example the UAE's PDPL, are still subject to sets of executive regulations which may have a bearing regarding how they are applied or enforced.

For this reason, it is understandable that businesses are in confused about when and how to follow some of the laws and regulations. This makes it difficult to know what resources within the business to allocate, and to determine what the cost of compliance will be.

Where enforcement is scant or non-existent, the cost of following complex rules or vague guidance may be difficult to justify within the business. But businesses should also keep in mind the consequences of regulatory sanction (even if it is not on the same scale as a penalty under the EU GDPR) or a data breach, which can go much further than a financial penalty. Reputational damage can have a severe impact on customer trust, and not just in the market where the breach or transgression happens.

With that in mind, we recommend that firms collecting and processing data in the region:

- adopt strong data protection policies and controls, whichever countries they operate in;
- base these on the 'gold-standard' frameworks you've implemented in jurisdictions with the most robust regulations;
- adapt their compliance plans where local rules demand more stringent measures.

In some cases, a business might find that doing so means it will be going beyond what's strictly necessary under the law in some markets. But this will also go a long way toward ensuring consistent compliance throughout the region.

Finally, make sure you seek expert advice in a region where there's significant complexity and legal uncertainty.

DLA Piper's Data Protection, Privacy and Security team in the Middle East has unrivalled knowledge of local data regulation. And we have specialist data-protection expertise in sectors that are burgeoning in the region, such as IT and communications.

Please get in touch to discuss how we support your organization's data compliance programme.

Carolyn Bigg
Partner
T +852 2103 0576
carolyn.bigg@dlapiper.com

Eamon Holley
Partner
T +971 4 438 6293
eamon.holley@dlapiper.com

Alex Mackay
Senior Associate
T +971 4 438 6160
alex.mackay@dlapiper.com