KPMG

The path toward robust personal data protection compliance

Practices for organizations in Saudi Arabia to comply with the new personal data protection law

August 2023
KPMG Professional Services

Contents

Foreword	3
The new law in practice	**4**
Challenges encountered by companies adopting privacy regulations	**8**
The next five years	**10**
Lessons to be learned, actions to be taken	**12**
References	15
Contacts	16

Foreword

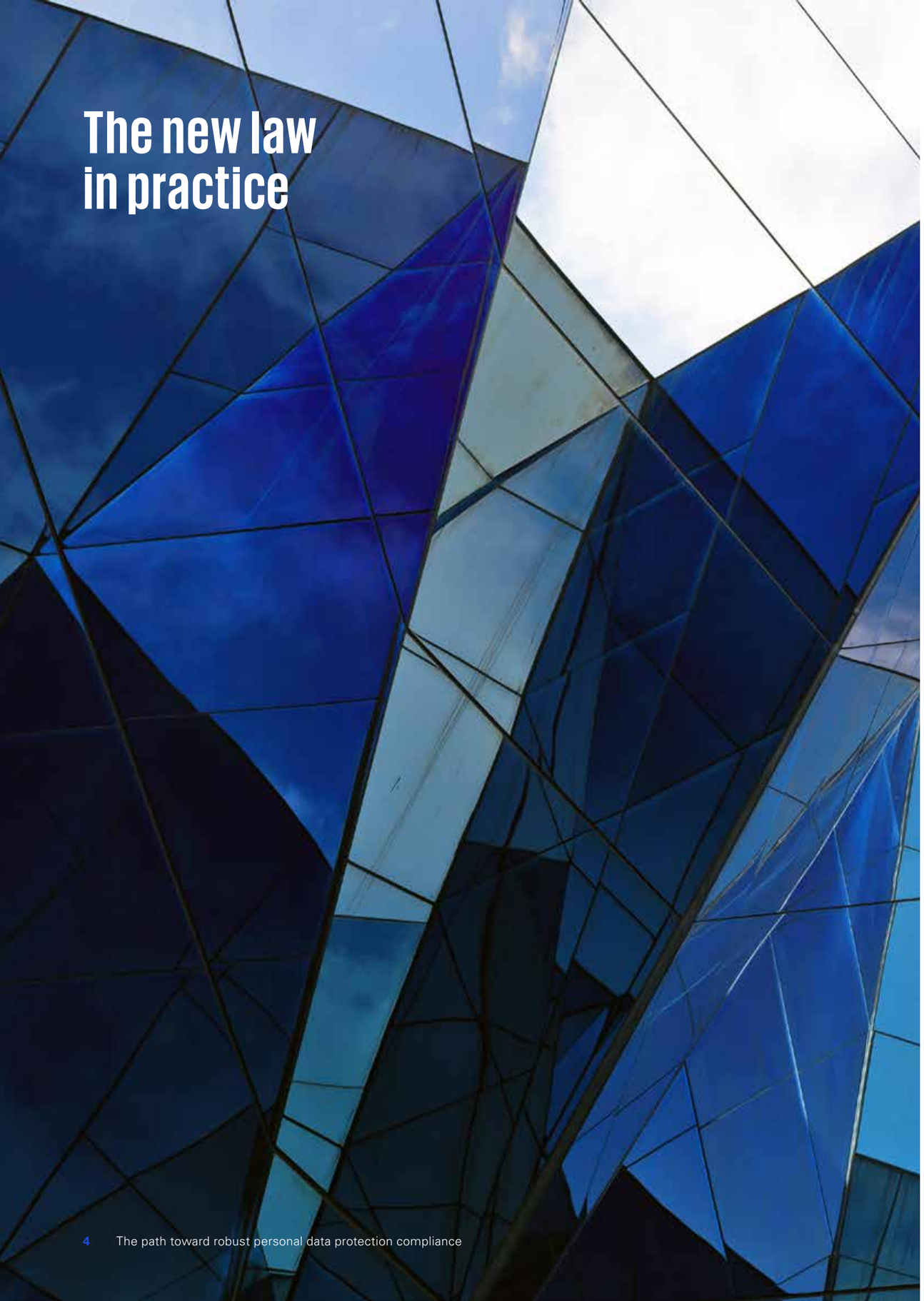
The much-anticipated Personal Data Protection Law (PDPL) was published in the Official Gazette on 24 September 2021. Following a recent review, PDPL will be formally active from 14 September 2023, marking a significant milestone in the Kingdom's commitment to privacy. The Saudi Data & Artificial Intelligence Authority (SDAIA), the presiding regulatory authority of PDPL, has granted businesses a one-year grace period starting from the law's enforcement date. This grace period, extending until 14 September 2024, offers a vital window of opportunity for organizations to fully comply with the provisions of the new law.

The introduction of the new law marks a significant development, considering the risks and venerabilities that businesses face in term of data privacy. The PDPL applies to all registered companies and sets out requirements around how businesses ought to collect, store, process, utilize, and dispose of personal identifiable information (PII), and in so doing can protect themselves and their customers. Additionally, the PDPL will require businesses to disclose any incidents where such personal identifiable information has been compromised within a certain timeframe.

In this paper, we aim to provide value insights for business in Saudi Arabia by observing the introduction of personal protection laws in other jurisdictions, particularly focusing on the introduction of the General Data Protection Regulations (GDPR) in the European Union (EU) in 2018. Drawing from these experiences, we hope to help them avoid potential pitfalls, penalties and reputational damage experienced elsewhere. Furthermore, we will investigate and predict the anticipated developments in this area over the next three years and beyond.

Ton Diemont
Head of Cybersecurity & Data Privacy

Ahmed Shokr
Data Privacy Lead



The new law in practice

Privacy and personal identifiable information pre-PDPL

Prior to the enaction of the PDPL, personal data was protected by the Shariah principles which dictated a rudimentary right of individuals to privacy and prohibited any action that may invade such privacy. Consequently, many businesses in Saudi Arabia are at an early stage in understanding the application, requirements, and potential consequences of the newly formalized, business-oriented legislation. This was born out by the need to extend the introduction of the law for a year to allow more time for companies in the Kingdom to prepare and put in place the required processes and protocols, to train and assign staff, and generally adopt a culture that would comprehensively protect the newly enforced data rights of individuals.

PDPL in comparative perspective

Saudi Arabia's PDPL bears similarities to the EU's GDPR across syntax, concepts, principles, and framework. The GDPR is one of the most comprehensive data protection laws in the world and has influenced many data protection laws in countries and jurisdictions far and wide, making it an exemplar for data privacy and protection laws throughout the world. Below are some of the main similarities between the GDPR and Saudi Arabia's new Personal Data Protection Law (PDPL):

Legal basis
Both laws are based on the principal that personal data can only be processed where there is a lawful basis to do so.

Data protection rights
Both laws uphold the right of data owners to be informed about how personal data are processed, obtain access to personal data and request correction and deletion of personal data.

Data protection
Both laws restrict data collection to relevant and essential-for-purpose information, prioritize adequate protection of personal data, and mandate risk assessment before processing.

Personal data privacy policy
Both law require consent before processing personal data and demand transparency in informing individuals about data processing purposes, collection methods, and data rights.

Notification of data breaches
Both laws stipulate that the regulatory authority should be notified about data breaches immediately. However, the GDPR sets a threshold in relation to the seriousness of the breach whereas the PDPL does not currently.

In some respects, the PDPL seems tighter in its administrative obligations and regulatory reach. An example is the extended requirement for separate consent of data use in specific situations, such as cross-border data transfer (CBDT) activities and the processing of sensitive personal information. This means companies will have the additional burden of determining, managing, and recording separate consent forms depending on different scenarios.

Another difference between the PDPL and the GDPR is the obligation of data controllers in Saudi companies to register with a separate authority responsible for managing registrations. At this stage, it is too early to determine whether registration represents a real or perceived increase in enforcement. However, companies would be advised to assume it is the former from the outset.

The PDPL places stricter requirements on companies and organizations transferring personal data out of Saudi Arabia. Cross-border data transfer (CBDT) is closely related to the kingdom's data localization laws. Companies are required to establish independent IT facilities or infrastructure in Saudi Arabia to isolate the data from other jurisdictions. Compared to the limitations on data flow between jurisdictions under the GDPR, CBDT in Saudi Arabia means that the PDPL is subject to stricter requirements which are not solely attributed to requirements under personal data law, but also to other laws and regulations associated with enforcing data localization. Additionally, the PDPL will apply to organizations and companies operating outside of Saudi Arabia that handle, manage and retain personal information on Saudi residents.

Avoiding hefty penalties

While the EU's data protection authorities can impose fines of up to €20 million, or 4 percent of worldwide turnover, whichever is higher, fines are structured and issued based on a company's international revenue.[1] In the first year, fines throughout the EU totaled €55.96 million which sounds like a large sum but was mostly made up of a single €50 million fine for Google.[2] However, this leniency in the first year of the GDPR was not a benchmark for preceding years; EU regulators have issued about $1.72 billion in fines for violations of the EU's GDPR since its effective date in May 2018.[3] Can companies in Saudi Arabia expect the same leniency from the regulator in the first year as was observed with the GDPR? That will have to be seen, but an assumption could be made that, just as with the EU's authorities, SDAIA will initially be lenient in the first year to penalize companies harshly where swift action is taken to correct misdemeanors. However, having said this, larger corporates may well fall under the same treatment as Google, and could face a severe penalty as an early example to encourage companies to comply with the new regulation. The sensible advice to all Saudi companies is to prepare for rigorous scrutiny from the outset with a strong likelihood that severe fines will be administered under the PDPL.

Regardless of the severity of the penalty applied, what is particularly relevant to companies based in Saudi Arabia is the potential damage caused to reputation, not only in terms of the reputational damage caused to the company, but also potentially to individual members of the Board and, in the case of family run businesses, the owner. To this point, the PDPL provides power to the court to request publication in a newspaper or other media stating non-compliance or data breach.

Another interesting point to note is that fines by EU authorities are imposed on companies of all sizes and for all types of misdemeanors, not just headline grabbing data breaches by larger corporations. In terms of the penalties process for the PDPL, the regulations outline only the principal rules, yet provide little detailed explanation of the procedures on how penalties will be imposed.

The top five GDPR fines*

Meta Platforms, Inc. (Facebook)
€1,200,000,000

Amazon Europe Core S.a.r.l.
€746,000,000

Meta Platforms Ireland Limited (Facebook)
€265,000,000

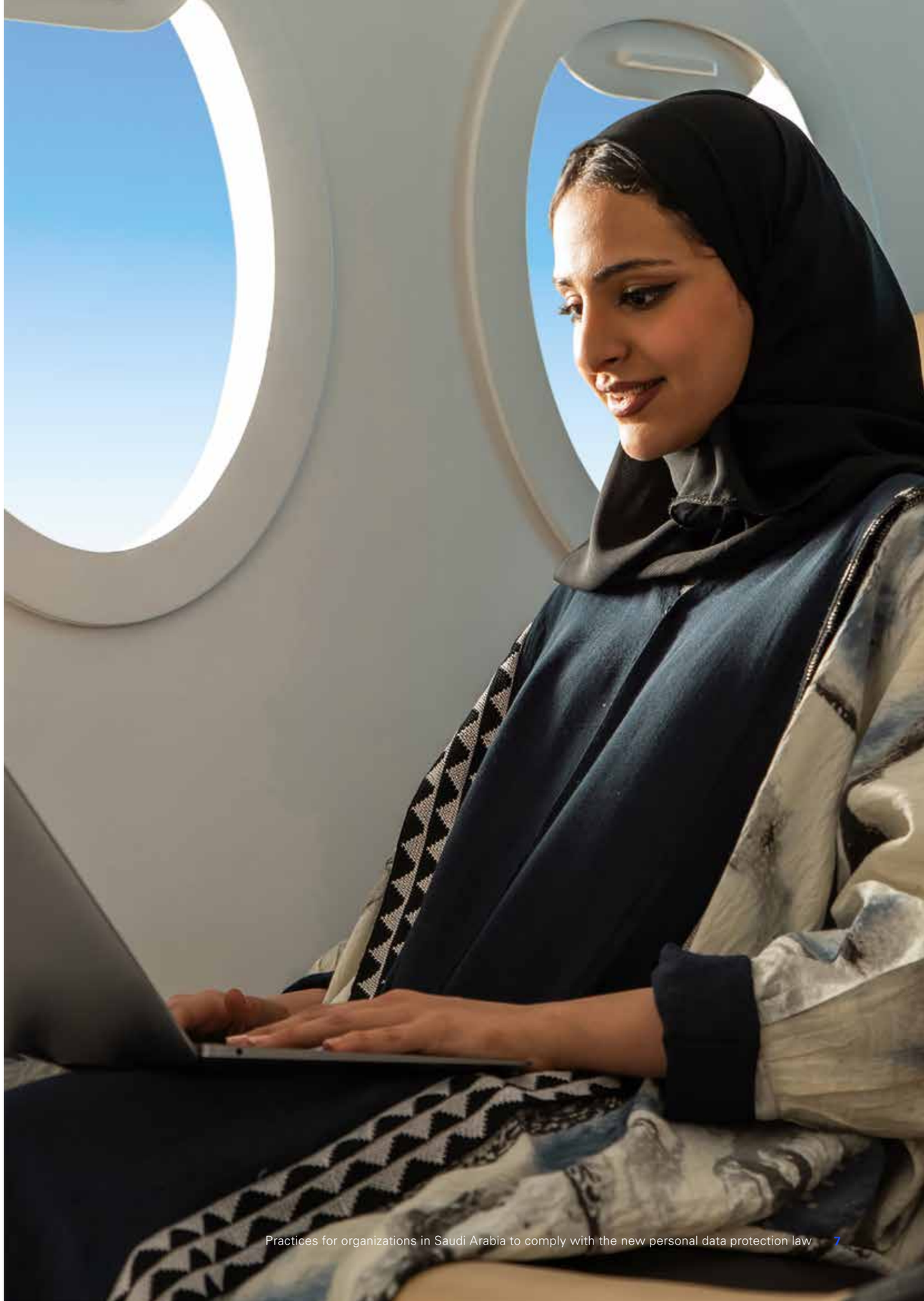
WhatsApp
€225,000,000

Google LLC
€90,000,000

*Only includes final and binding fines, June 2023.

PDPL fines and penalties

Disclosure or publication of sensitive personal data in violation of the PDPL (including data breach)	Imprisonment for up to two years and a fine of up to SAR3,000,000
Violation of data transfer provisions (including cross-border data transfers)	A fine of up to SAR1,000,000
All other breaches of the provisions of the PDPL	Warning notice or a fine of up to SAR5,000,000
Repeat offenses	Double the stated maximums above



Challenges encountered by companies adopting privacy regulations

Following the launch of the GDPR several persistent challenges emerged, the most common are the following.

Comprehensive, companywide system audit and assessment

Because PII is used across many departments, business units and processes within an organization, many companies realized the need to undertake a thorough audit and assessment of information systems as part of their GDPR adoption strategy.

Privacy by design training

With the introduction of the GDPR, many companies undertook an approach of overhauling or developing new systems and processes to incorporate privacy safeguarding features. Companies would be well-minded to adopt a similar approach.

Cultural transformation

Many companies found to their cost that adopting the GDRP went beyond simply having a data protection policy and framework in place and required a cultural shift across the entire organization. Focusing on prioritizing the continuous safeguarding of personal data required a shift in culture for European companies and the same will be true for many organizations in Saudi Arabia wanting to embed a culture of data protection into their organizations.

Technical challenges

The increasing uptake in cloud services resulted in a significant increase in the volume of personal data being collected and stored. This in turn dramatically increased the amount of data to secure and manage which was added to by the GDPR requirement to hold customer data securely, provide data access for data subjects when required, and to only retain data as long as truly necessary. This means that firms need to have a good understanding of all the personal data they hold. However, we see firms often not being able to pin down where personal data lives in their cloud environment or how it is processed. This makes it very difficult to fulfil their obligations under the GDPR requirements for data subjects right of access and deletion. To overcome this, firms should look to specialised technology partners to implement retention effectively, properly inventory and manage the data in the cloud environment and determine the applicable laws based on its location.

Revised budget planning

GDPR is an additional cost burden to companies, requiring budget planning and auditing to ensure cost impacts are kept within acceptable levels.

Multi-level compliance training

GDPR compliance touches most areas and operations of a business to varying degrees. Consequently, companies in the EU adopted the practice of requiring all staff dealing with personal data to attain a basic level of compliance training, and identified specific areas, departments and individuals for additional advanced compliance training where needed. In Saudi Arabia, data controllers will be required by law to train staff on the terms and principles of the PDPL. Companies would be well advised to adopt a similar approach to that of companies in the EU to minimize the cost of extensive training programs while ensuring compliance.

Responding to user requests in a timely manner

Under the GDPR, the response deadline for user information requests is 30 days. The law grants various rights to individuals (data owners), including the right to be informed, the right to access data collected about them, the right to request correction, completion or updating of their personal data and the right to request deletion of data. Companies and businesses operating within sectors requiring extensive data to be held on large numbers of customers are presented with a considerable additional burden in processing information requests within short timeframes. The information deadline for the PDPL is also 30 days and the rights of data owners are equally comprehensive in scope with similar implications and impacts for companies anticipating a high frequency of information requests.

The next five years

As a piece of legislation, the PDPL is not only a pillar of citizen empowerment and an enabler for Saudi Arabia's digital transition, but also a measured response to the current context in which businesses operate, providing guidance as well as enforcement to navigate a dynamic market driven by data and digital transition. Within this dynamic context, the PDPL is likely to undergo further updates and refinement over time and companies will need to maintain vigilance to maintain compliance and keep up to speed of any changes.

Regardless of attitudinal differences between the EU and Saudi Arabia towards personal data, there is a strong likelihood that consumers will become more privacy-conscious in the kingdom. According to a survey published in 2020 by the European Commission (two years on from the law's introduction), 69 percent of the EU population above the age of sixteen had heard about the GDPR and 71 percent of people in the EU knew about their national data protection authority.[4]

A greater awareness and knowledge of data privacy and protection issues, coupled with a drive towards best practice, was found to cause a rise in reported data breaches resulting from whistleblowers and increased numbers of complaints by citizens. It is likely, therefore, that lawmakers and regulators will respond by broadening privacy laws and enforcing them with greater stringency in the future.

While the initial focus will be on local businesses becoming PDPL-compliant, there will eventually be a requirement for organizations located outside the Kingdom that process the personal data of Saudi constituents to comply with the PDPL. Currently, this requirement has been deferred for a period of up to five years from the law's introduction. However, companies would be well advised to prepare for this eventuality in good time for the sake of business continuity.

Lessons to be learned, actions to be taken

The comparison and observations of the GDPR outlined here provide a clearer view of some of the challenges and potential outcomes resulting from the introduction of the PDPL over the forthcoming months and years as the new law is adopted and becomes embedded. From these observations, robust compliance from the start will enable companies in Saudi Arabia to avoid the pitfalls encountered by counterpart companies in the EU with the GDPR. What is clear is that having a plan in place sooner rather than later is preferable than simply delivering a minimum level of compliance and hoping it will be enough. The likelihood is that it won't, as so many companies have found to their cost.

Preparing the ground

- **Getting to know the new regulation**
  Understanding the law and the specific implications and risks to the business.

- **Assessing existing business activities and making plans to align with the PDPL**
  In some instances, companies may have to completely review their operations within the context of compliance with the provisions of the PDPL.

- **Assessing the potential negative impact for non-compliance**
  Detailing on a new line scenarios where poor handling of personal data could cause or compound loss to the business.

- **Seeking expert advice on complex data protection law with entities outside Saudi Arabia**
  Some businesses may be aware of strict data protection requirements when dealing or doing business in or with other territories where stringent data protection laws apply, while not applying those same rules, protocols, and constraints to data within the kingdom. In these instances, an integrated privacy law framework will be required.

Putting compliance at the heart of the business

The next phase involves executing the plans, establishing policies, setting protocols, and developing the tools, personnel, and companywide culture to ensure a compliance with the PDPL. Specific actions should include the following.

- **Assigning a data controller**
  Companies should assign a data controller who will be wholly responsible for the management of PII within the organization. A recent amendment to the PDPL means there is no longer a requirement for controllers to be registered or to disclose their processing activities.

- **Setting up a compliance taskforce**
  This will require additional training of staff and potentially new hires where specialist skills are determined to be lacking.

- **Drafting and setting out a strong privacy controls framework**
  To be applied across the entire business.

- **Drafting new policies**
  These will help to govern how people within your organization process personal and sensitive data.

- **Reviewing and updating contracts**
  Existing contracts will require redrafting, considering changes in rights and obligations under the provisions of the PDPL.

- **Educating staff and key stakeholders**
  On PDPL compliance requirements, personal data protection standards and best practice, and obligations on obtaining consent, amongst others.

- **Actively enforcing data protection**
  Additional training may be required across all business units, departments, and operations, top to bottom.

- **Managing third party data ecosystem vulnerabilities**
  Vendors and suppliers should be included in every business' PDPL planning. Using third parties is an extension of the company's IT environment without necessarily retaining the control of it.

Achieving sustained compliance

PDPL compliance is ongoing and doesn't simply apply to the current state of the business. Therefore, a program of continuous management and maintenance is required. From the experience of businesses with the GDPR, the PDPL is likely to evolve over time with additional amendments, reviews and modifications anticipated following the introduction of the new law. Consequently, data controllers and plan managers must be vigilant for further changes, amendments, and updates to ensure full PDPL compliance. Similarly, new and evolving technologies, tools and processes must align with the law to ensure compliance is maintained.

The benefits of robust PDPL compliance

One question that every manager responsible for data handling and processing should ask themselves is this: would I be happy to trust my personal data with my company if I were a customer or client? Establishing a strong PDPL deployment and continuous compliance management program from the outset will ensure customer trust and loyalty is maintained. Business loss resulting from hefty penalties and the potential of loss of customers or clients can be mitigated through robust data protection and compliance.

Lastly, establishing a strong PDPL deployment and continuous compliance management program will help to mitigate the potential loss of corporate or business reputation and in some sectors, it could even help prevent a critical loss of business. For example, within banking and finance, a license to operate could be rescinded by the Saudi Central Bank (SAMA) in extreme or persistent cases. Therefore, implementing a strong PDPL deployment and continuous compliance becomes an essential strategic move to ensure long-term success and sustainability in today's data-driven business landscape.

At KPMG, our team of data privacy experts work closely with companies across all sectors to help them develop, maintain, and achieve compliance with Saudi Arabia's new personal data protection law.

For more information on how to achieve full PDPL compliance through a robust and sustained privacy framework, please get in touch.

References

Endnotes

[1] 2021 in GDPR fines | International Network of Privacy Law Professionals, 2022 https://inplp.com/latest-news/article/2021-in-gdpr-fines/.

[2] GDPR four years on: €1.6bn in fines but still a work in progress. Techmonitor, June 2022. https://techmonitor.ai/policy/privacy-and-data-protection/gdpr-fines-four-years-work-in-progress.

[3] GDPR fines tracker and statistics. Privacyaffairs.com, 2023. https://www.privacyaffairs.com/gdpr-fines/.

[4] Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation (2020). EUR-Lex - 52020DC0264. Communication from the Commission to the European Parliament and the Council. EUR-Lex https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264.

Recommended sources

Data Protection Laws and Regulations Saudi Arabia 2022-2023. https://iclg.com/practice-areas/data-protection-laws-and-regulations/saudi-arabia.

Saudi Arabia's Personal Data Protection Law (PDPL). https://www.cookieyes.com/blog/saudi-arabia-personal-data-protection-law/.

Saudi Arabia PDPL Compliance: How to Prepare | BigID. https://bigid.com/blog/saudi-arabia-pdpl-compliance/.
How to prepare for Saudi Arabia's Personal Data Protection Law. https://iapp.org/news/a/how-to-prepare-for-saudi-arabias-personal-data-protection-law/.

Privacy and Data Protection in Saudi Arabia. Gov.sa. https://www.my.gov.sa/wps/portal/snp/content/dataprotection/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfljo8zijQx93d0NDYz83UNCjA0CvZz8Q4OdTV2Ng831g1Pz9AuyHRUBCMR-8g!!/.

Comparing Privacy Laws: GDPR v. Saudi Arabia's PDPL. https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-saudi-arabias-pdpl.

Saudi Arabia's New Personal Data Protection Law – GDPR similarities and differences. https://cms-lawnow.com/en/ealerts/2021/10/ksa-s-new-personal-data-protection-law-gdpr-similarities-and-differences.

Saudi Arabia confirms updates to the Personal Data Protection Law. https://www.clydeco.com/en/insights/2023/04/saudi-arabia-confirms-updates-to-pdpl.

Saudi Arabia's PDPL | Portal Advisory | DataGuidance. https://www.dataguidance.com/advisories/saudi-arabia-pdpl.
The Two Key Challenges of GDPR Adoption - ISACA. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/the-two-key-challenges-of-gdpr-adoption.

Challenges and Benefits of GDPR Implementation - The APP Solutions. https://theappsolutions.com/blog/development/gdpr-challenges-and-benefits/.

Contacts

Ton Diemont
Head of Cybersecurity &
Data Privacy
E: antondiemont@kpmg.com

Ahmed Shokr
Data Privacy Lead
E: ashokr@kpmg.com

kpmg.com/sa