Evolving personal data protection requirements

Following a one-year compliance grace period, Saudi Arabia's Personal Data Protection Law (PDPL) is now in place and coming into force on 14 September 2023, with the enforcement deadline set for 14 September 2024. The new law regulates the processing of personal data in Saudi Arabia and applies to any entity that processes personal data of individuals within the Kingdom.

The PDPL is the first comprehensive generally applicable data protection law in Saudi Arabia and shares similarities with the best practice data protection laws from around the world, such as the EU's General Data Protection Regulation (GDPR). Based on broad principles covering consent, transparency, lawfulness, and purpose limitation, the PDPL is straightforward for most companies to comply with, however, certain sectors involved in providing services that require the frequent handling of large amounts of personal data will find PDPL has a greater impact.

For the banking and financial services industry, compliance with PDPL will present additional requirements, a need for tighter internal controls, and the setting of new policies and protocols. While most requirements are administrative in nature, the PDPL does impose general obligations on data controllers (and the entity) to ensure the security, accuracy and confidentiality of personal data which can extend to IT infrastructure, systems, and policy layers.

The new law also requires the provision for expanded rights of citizens concerning their personal data and how it is managed by the bank or financial entity, which include:

Consent

The PDPL requires data controllers to obtain consent from data subjects before processing their personal data unless an exception applies.

Actionable data rights for citizens

This includes but is not limited to the right to access, right to correct, and right to delete personal data. This will require the setting up, reconfiguration and maintenance of storage and retrieval systems.

Restrictions on personal data transfer

Including transferring data outside of Saudi Arabia unless certain conditions are met. Certain types of transfer are exempt from the conditions, such as when an individual has consented to the transfer or where the transfer is necessary to fulfill an agreement.

PDPL compliance challenges

The PDPL requires companies to comply with various obligations, such as appointing a data protection officer, conducting data protection impact assessments, notifying data breaches, and obtaining prior approval for cross-border data transfers. The additional burden on individual companies will depend on their size and the current sophistication of existing data handling operations. For the banking industry, there is likely to be minimal impact in this regard, however, there will be the need for a degree of on-the-job training, along with modification, or upgrading legacy systems to ensure compliance.

“ Any bank processing personal data in Saudi Arabia must aim for full PDPL compliance and keep a close eye on further guidance from the regulator.

As with any new law of this kind, there will be a period of 'bedding in' where rules are assimilated, adjustments are made, and definitions are refined. Some examples where this could occur might be in differentiating between personal data and sensitive personal data; deciding what minimum data should be requested at each stage of customer interaction; and which criteria should be applied for consent and legitimate interest and when. There will be many other areas where judgement on compliance will need to be considered as the law becomes established.

Violations, penalties, and enforcement

Banks and financial institutions and companies failing to comply fully with the PDPL could receive a fine of SAR3 million (US$800,000) or imprisonment for up to two years.[1] In exceptional circumstances or where an entity persistently fails to comply, SAMA could see fit to suspend or retract banking licenses.

It is not yet clear how claims of non-compliance regarding personal data protection will be made and dealt with, however, it is likely that citizens will be directed to the Ministry of Commerce and an official reporting and complaint handling process will be established over time.
Where a data security breach is detected, under the PDPL, controllers are obliged to notify the relevant authority. The PDPL enforces penalties for disclosure or publication of sensitive personal data that can include a fine not exceeding SAR3 million and/or imprisonment for up to two years. Penalties in relation to violations regarding data transfers include a fine not exceeding SAR1 million and/or imprisonment for up to one year. For violations of other provisions of the PDPL, penalties are limited to a warning notice or a fine not exceeding SAR5 million.

Ultimately, the PDPL is designed to help protect the privacy of individuals in Saudi Arabia, and to ensure that banks processing personal data are held accountable through a system of severe penalties. More importantly, however, any bank or financial entity breaching PDPL regulations involving the collection, usage, transfer, or storage of personal data, whether intentional or not, risks reputational damage.

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