DENTONS GLOBAL ADVISORS | ASG ALBRIGHT STONEBRIDGE GROUP

ASG ANALYSIS:

New Changes to Saudi Arabia's Personal Data Protection Law

Key takeaways

- On April 4, Saudi Arabia's Council of Ministers published a long-awaited list of changes to the Kingdom's Personal Data Protection Law (PDPL).
- The original PDPL was published in September 2021, but its entry into effect was delayed by a full year in March 2022 to allow for revisions – reportedly in response to feedback from industry players and key Saudi regulators (see our previous Analysis).
- Most importantly for companies doing business in the Kingdom, the revised PDPL outlines a broader set of circumstances under which cross-border data transfers are allowed. It also introduces standard "data adequacy" language, mandating that data can only be transferred to jurisdictions offering equal or higher levels of data protection, although the law does not specify the process or criteria for making adequacy decisions.
- Other key changes include a narrower definition of sensitive data (notably excluding credit data), as well as stricter individual data privacy rights and consent requirements.
- The revised PDPL, even more than the original version, appears to be broadly aligned with the European Union's General Data Protection Regulation (GDPR), although it still allows a greater role for national security interests.
- The implementing regulations, which we expect will provide further clarity on how key provisions will be defined and enforced in practice, must be issued by September 6, 2023 (720 days from the date the original law was published), and companies will have one year after that to comply.
- We expect draft versions of the implementing regulations to be issued for public consultation. Companies should seize this opportunity to engage with key regulators such as the Saudi Data and Artificial Intelligence Authority (SDAIA) to advocate for their data needs and shape the final regulations.

Key changes to the PDPL

Based on a high-level comparative analysis of changes to the PDPL and the original law, we have identified key changes that allow companies greater flexibility: changes to provisions regarding cross-border data flows and a new definition of sensitive data.

Cross-border data flows

Article 29, concerning cross-border data transfers, is arguably the most important provision for organizations doing work in and with the Kingdom. The original law only allowed cross-border data flows if: 1) the transfer of data did not threaten the vital interests of the Kingdom; 2) the receiving entity provided sufficient safeguards to preserve personal data; and 3) the transfer or disclosure of data was limited to the minimum amount of personal data needed. In short, the clauses both lacked specificity and sharply limited the transfer of data across borders.

The revised Article 29 outlines a broader set of circumstances under which cross-border data transfer is allowed, including: 1) if the disclosure is mandated under an agreement to which the Kingdom is party; 2) if the disclosure fulfils an obligation to which the individual data subject is party; 3) if the disclosure serves the interest of the Kingdom; or 4) "other purposes" to be specified in the implementing regulations.

The revised article also introduces standard adequacy language as seen in the GDPR, mandating that data may only be transferred outside of the Kingdom if the country or entity to which the data is being transferred offers an "appropriate level" of personal data protection equal to or more stringent than the Saudi PDPL.

The revised law does not specify which jurisdictions it considers suitable for cross-border data transfers or the criteria on which an adequacy decision would be based. However, it outlines a general process where SDAIA, as the competent authority, would need to conduct a review of the level of protection offered by the laws and regulations of the receiving jurisdiction(s) and present that review to the prime minister. The implementing regulations will further clarify the level of protection needed.

Sensitive data

Another key change to the PDPL is the updated definition of sensitive data. Sensitive data now includes: any reference to an individual's racial or ethnic origin, or to their religious, intellectual, or political belief; any security and criminal data; any biometric data that identifies the individual's identity, or genetic data; any health data; and any data indicating that an individual is of unknown parents. It notably does not include credit data (including bank accounts and credit card numbers), providing data controllers (particularly e-commerce and financial institutions) with greater flexibility to conduct international business and transactions.

Other key changes

Other key changes to the law include:

- **Expanded data privacy rights for the individual.** According to the updated PDPL, the individual has the right to be informed of the reason for collection of personal data; the right to access their personal data; the right to correct, complete, or update their data; and the right to request that their data to be erased.

- **Stricter consent requirements.** The revised law mandates that the controller cannot disclose personal data except if: the individual consents to the disclosure of data; the individual's data is collected from a publicly available source; the entity requesting disclosure is a public entity requesting the data for security purposes; the disclosure of data is necessary to protect the public health, safety, interest, or life of a specific individual; the disclosure does not identify the individual; or the disclosure is necessary to achieve the lawful interest of the data controller. (We expect that the implementing regulations will further clarify what constitutes a necessary disclosure.)

- **Limitations on obtaining data from third parties.** Unlike the previous version of the PDPL, which allowed the data controller broad rights to request data from third parties, the revised law says that the data controller can only obtain data directly from the individual (except when in the lawful interest of the data controller).

Comparing the PDPL and GDPR

The revised PDPL, even more so than the original version, appears to be broadly aligned with the European Union's General Data Protection Regulation (GDPR). Key similarities between the PDPL and the GDPR include similar data protection rights and principles, the reliance on fines as an enforcement tool, and strict regulations regarding cross-border data transfers (though the GDPR has a more established process and criteria for adequacy decisions regarding cross-border data transfers, while the PDPL does not yet provide this level of detail).

A key difference between the PDPL and GDPR is that the PDPL broadly treats data transfers as an issue of national security, noting the involvement of national security bodies such as the Ministry of Foreign Affairs and the National Cybersecurity Authority. The GDPR, on the other hand, is less focused on national security and more focused on protecting the rights of individuals.

Key dates and next steps for companies

Companies operating in the Kingdom should be aware of three key dates:

- **September 6, 2023**: The implementing regulations must be published within 720 days from the date the original law was issued.
- **September 14, 2023**: The new law will enter into force 720 days from the date the original law was published in the official gazette.
- **September 3, 2024**: Companies must comply within roughly one year after the law enters into force.

Before the implementing regulations are released, it is likely that SDAIA will issue public consultations for implementing regulations. To prepare for these public consultations, companies should:

- **Closely review the changes to the PDPL** and compare them side-by-side with the original law;
- **Identify data needs and build plans** to implement changes to current data practices as mandated by the PDPL;
- **Partner with peer companies** to exchange knowledge and best practices; and
- **Proactively engage with regulators** to advocate for data needs and shape the development of the implementing regulations.

About ASG

Albright Stonebridge Group (ASG), part of Dentons Global Advisors, is the premier global strategy and commercial diplomacy firm. We help clients understand and successfully navigate the intersection of public, private, and social sectors in international markets. ASG's worldwide team has served clients in more than 120 countries.

ASG's Middle East and North Africa practice has extensive experience helping clients navigate markets across the Middle East. For questions or to arrange a follow-up conversation please contact Juliana Rordorf.