Kingdom of Saudi Arabia Approves Amendments to Personal Data Protection Law and Confirms September 2023 Effective Date

By Natasha G. Kohne, Sahar Abas, Abdulaziz Al Moosa and Mazen Baddar

April 26, 2023

On March 27, 2023, the Kingdom of Saudi Arabia (KSA) Council of Ministers approved a series of 27 amendments (the Amendments) to the KSA Personal Data Protection Law (PDPL) pursuant to Royal Decree No. M148 of 05/09/1444H (the text of the Amendments is available in Arabic only **here** and the text of the consolidated PDPL reflecting the Amendments is available in Arabic only **here**). The PDPL constitutes the country's first comprehensive national data protection legislation and was initially published on September 24, 2021, pursuant to Royal Decree M/19 of 9/2/1443H. Since its initial publication, there have been a series of developments, including the Saudi Data and Artificial Intelligence Authority (SDAIA) announcing that full enforcement of the law had been postponed, the issuance of draft executive regulations supplementing the PDPL and a public consultation on proposed amendments to the PDPL by the SDAIA in November 2022 (as to which see our previous blog post **here**). The Amendments reflect some, but not all, of the amendments proposed in the public consultation, as further discussed below.

The PDPL regulates the processing of personal data relating to an individual in the KSA by any means, including where such processing is conducted by a party outside the KSA, and further establishes certain novel rights for individuals in relation to how their personal data is processed by data controllers (with consent being at the forefront), and creates new obligations for data controllers to adhere to. Following the approval of the Amendments, organizations operating in the KSA should promptly begin taking practical steps to ensure compliance. While compliance with existing international data protection laws, such as the European Union's General Data Protection Regulation (GDPR), may be beneficial, the unique features of the PDPL must be taken into consideration.

The Amendments implement significant amendments to the previous version of the PDPL, notably including:

- **Amendment of Definitions**: The Amendments amend a number of definitions in Article 1 of the PDPL, including narrowing the definition of "Sensitive Personal Data" by removing the prior references to membership in a civil association or institution, credit data and location data (and instead now referring solely to personal data relating to an individual's ethnic or racial origin, religious, intellectual or political belief, criminal and security data, biometrics data, genetic data, health data and data indicating that one or both parents of an individual is unknown), and amending the definition of "Owner of Personal Data" to remove the previous extension to an individual's legal representative or guardian (such that it now refers only to the individual to whom the personal data relates).
- **Written Consent vs. Explicit Consent**: The Amendments no longer require consent to be in writing, instead requiring consent to be "explicit."
- **Legitimate Interests Lawful Basis**: One of the most significant amendments approved by the Amendments is the inclusion of legitimate interests as a lawful basis for processing data, although the term is not further defined under the PDPL. Pursuant to the Amendments, (1) the processing of personal data under the PDPL is not subject to the requirement for consent in Article 5 of the PDPL where the processing is necessary to

achieve the legitimate interests of the controller, and (2) a controller may collect personal data directly from a person other than the owner or may process such data for purposes other than the purpose for which it was collected where such collection or processing is necessary to achieve the legitimate interests of the controller, in each case unless such processing prejudices the rights of the owner of the personal data or conflicts with their interests and provided such data is not sensitive personal data. Furthermore, whereas a data controller could previously only disclose personal data in five prescribed circumstances, the Amendments now also permit disclosure if it is necessary to achieve the legitimate interests of the controller, provided such disclosure does not prejudice the rights of the owner of the data, conflict with their interests or constitute sensitive personal data.

- **International Data Transfers**: Another significant amendment approved under the Amendments is the extension of the data transfer provisions. Previously, data controllers were prohibited from transferring personal data outside of the KSA (except in cases of extreme necessity to preserve the life of the data subject outside of the KSA or their vital interests, or to prevent, examine or treat a disease), unless such transfer was in the implementation of an obligation under an agreement to which the KSA was a party or to serve the interests of the KSA and only after four prescribed conditions were met, including the approval of the competent authority for the transfer or disclosure. Pursuant to the Amendments, a data controller may transfer personal data outside of KSA in order to achieve certain prescribed purposes (retaining the two previous grounds under the initial draft of the PDPL, namely to serve the interests of the KSA or in the implementation of an obligation under an agreement to which the KSA is a party, and the exception for cases of extreme necessity, the vital interests of the data subject and relating to disease), notably now including if it is in implementation of an obligation to which the owner of the personal data is a party and if it is in implementation of other purposes specified in the regulations (which were previously not grounds on which a data transfer was permissible). The conditions that must be met when transferring or disclosing personal data outside of the KSA are further confirmed (retaining the previous requirement that the transfer should be limited to the minimum amount of personal data required and that the transfer shall not prejudice the national security or vital interests of the KSA), although the requirement to seek the approval of the competent authority in respect of the transfer or disclosure has now been removed and the Amendments now include the requirement that there shall be an appropriate level of protection for the personal data outside of the KSA (which must not be less than the level of protection stipulated in the PDPL and the associated regulations—previously the PDPL required that sufficient guarantees be provided to preserve the personal data being transferred and for the confidentiality of such data to be preserved at a standard not less than that stipulated by the PDPL or the regulations). The executive regulations supplementing the PDPL shall specify the provisions, standards and procedures relating to the application of the data transfer provisions, including determining the circumstances in which a controller may be exempt from compliance with any of the prescribed conditions.
- **Repeal of Electronic Register Requirement**: The Amendments repeal Article 32 of the PDPL, which previously provided that the competent authority shall establish an electronic portal for the purposes of building a national register of controllers and requiring all data controllers to register in the portal.
- **Data Breach Notification**: Previously, if the leakage of, damage or unauthorized access to personal data would cause serious harm to the personal data or the owner of the personal data, the controller was required to notify such person "immediately." This timing requirement has been removed under the Amendments; instead, a controller must notify the owner of personal data of any leak, damage or unauthorized access to personal data that may result in damage to such data or conflict with the person's rights or interests, as shall be further specified in the regulations.
- **Penalties for Non-Compliance**: Previously, any person found to violate the data transfer provisions of Article 29 of the PDPL was subject to punishment by imprisonment for a period not exceeding one year and/or a fine

not exceeding 1,000,000 Saudi Riyals. The Amendments no longer include this penalty, but retain the penalty of imprisonment for a period of two years and/or a fine not exceeding 3,000,000 Saudi Riyals where a person discloses or publishes sensitive personal data in violation of the PDPL (where such disclosure or publication is made with the intention of harming the owner of the data or achieving a personal benefit). Administrative fines of up to 5,000,000 Saudi Riyals may also be issued for any other violation of PDPL.

- **New Effective Date**: Pursuant to the Amendments, the PDPL shall now enter into force 720 days after the publication of the original law in the KSA Official Gazette such that the PDPL shall be effective from September 14, 2023. However, data controllers have a one-year grace period in order to comply with the PDPL (i.e., September 14, 2014). Executive regulations supplementing the PDPL are due to be issued in advance of this effective date and will likely provide further detail and clarification as to the provisions of the PDPL.

As the effective date approaches, businesses that are required to comply with the new PDPL should start examining their data processing activities, including any cross-border data transfers, to ensure timely compliance with the PDPL. To achieve this, businesses may want to:

1. Create or update existing policies and procedures related to data protection.
2. Provide training for employees on the key provisions and significance of the PDPL.
3. Appoint a data protection officer to oversee compliance efforts (noting that the PDPL expressly states that the executive regulations shall specify the circumstances in which a controller must appoint or designate a person as a personal data protection officer).
4. Conduct regular audits and assessments of data protection practices.
5. Implement privacy-by-design and privacy-by-default principles in new projects and systems.
6. Establish a process for handling data subject requests, such as data access, rectification, or deletion.
7. Develop a clear procedure for reporting data breaches to the appropriate authorities.
8. Regularly update and review data protection measures to maintain compliance with the evolving legal landscape.

If you need assistance with complying with the new PDPL or implementing any of the actions mentioned above, please do not hesitate to reach out to our team for support and guidance.

We continue to monitor developments in this area.

If you have questions about this client alert, please contact any Akin lawyer or advisor below:

Natasha G. Kohne
nkohne@akingump.com
+1 415.765.9505

Sahar Abas
sabas@akingump.com
+1 971.317.3052

Abdulaziz Al Moosa
aalmoosa@akingump.com
+1 971 4.317.3077

Mazan Baddar
mbaddar@akingump.com
+1 971 2.406.8552
