ARTICLE • JUNE 2025

SAUDI ARABIA'S PERSONAL DATA PROTECTION LAW: A COMPREHENSIVE OVERVIEW OF THE LEGAL AND REGULATORY FRAMEWORK

THE DIGITAL ECONOMY POLICY AND SDAIA'S ROLE

In alignment with Vision 2030, the Kingdom of Saudi Arabia approved its Digital Economy Policy through Council of Ministers Resolution No. (267) dated 14/05/1442H. The Policy underscores the Kingdom's ambition to rank among the top 15 global economies by 2030, recognizing data as a central enabler of innovation, economic development, and effective governance.

Data is classified as a key pillar of the digital economy, enabling innovative solutions and informed decision-making. The Policy emphasizes the responsible collection, use, and sharing of data in accordance with national data protection legislation, prominently including the Personal Data Protection Law (**PDPL**).

The Saudi Data and AI Authority (**SDAIA**), established by Royal Order No. (A/471) dated 29/12/1440H, is the Kingdom's lead agency for all matters relating to data and artificial intelligence. SDAIA, headquartered in Riyadh and reporting directly to the Prime Minister, operates with financial and administrative independence and oversees three sub-entities: the National Data Management Office (**NDMO**), the National Center for AI (**NCAI**), and the National Information Center (**NIC**). SDAIA's core responsibilities include issuing data regulations, fostering innovation, and building Saudi Arabia's leadership in the global digital economy.

THE DEVELOPMENT OF THE PDPL AND ITS REFORMS

Initially issued in September 2021, the PDPL underwent substantial amendments and was reissued under Royal Decree No. (M/148) dated 05/09/1444H. The amended PDPL came into force on September 14, 2023, with a one-year grace period granted to entities for compliance, ending on September 14, 2024.

KEY AMENDMENTS INTRODUCED BY THE REFORM

Definitions and Sensitive Data Classifications

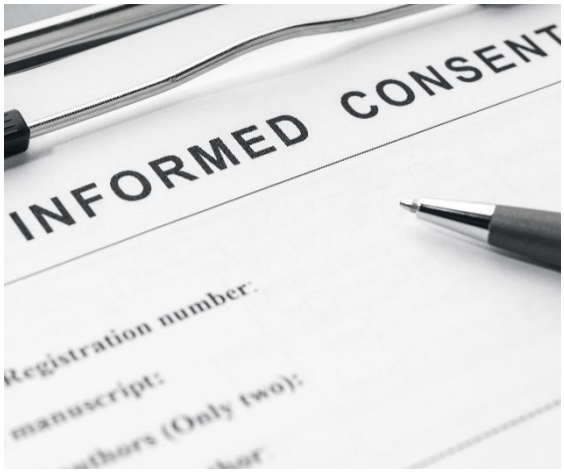
- Introduction of the definition of "destruction of personal data" as any act that makes access to or identification of the data or its subject impossible.
- Removal of civil society membership and tribal affiliation from the list of sensitive personal data.
- Narrowing the definition of "personal data subject" to refer only to the individual concerned, excluding representatives or guardians.

Consent Requirements

The requirement for written consent has been replaced with the requirement for "explicit" consent, allowing more flexibility in the form of authorization.

Cross-Border Data Transfers

- International transfers or disclosures of personal data under specific conditions—including compliance with international obligations, national interest, or contractual obligations—have been permitted.
- The prohibition of transfers that threaten national security or infringe on privacy rights.
- Prior approval from the authority is no longer required, but the authority maintains the power to regulate or exempt these transfers, including sensitive data.



ENFORCEMENT MECHANISMS AND CYBERSECURITY INTEGRATION

Saudi Arabia has implemented a comprehensive framework to address cybersecurity threats alongside data protection obligations.

Anti-Cyber Crime Law (ACCL)

Enacted under Royal Decree No. (M/17) in 2007, the ACCL defines cyber offenses such as unauthorized access, cyber fraud, defamation, and dissemination of illegal content. Penalties range from fines to multi-year imprisonment depending on severity.

Enforcement is shared among:

- The Ministry of Interior and security agencies for investigations;
- The Public Prosecution for prosecution; and
- The Communications and Information Technology Commission for technical support.

National Cybersecurity Authority (NCA)

NCA issues mandatory Essential Cybersecurity Controls (ECCs) and houses the Saudi Computer Emergency Response Team (Saudi CERT). It ensures national cyber resilience, particularly in critical sectors.

Sectoral Oversight

- The Saudi Central Bank (SAMA) enforces a cybersecurity framework for financial institutions.
- The CITC oversees cybersecurity in the telecom sector.

SAMA has also issued detailed PDPL compliance directives to financial institutions, including:

- Updating internal policies by the end of the grace period;
- Submitting semi-annual compliance reports; and
- Using SAMA as the central liaison with SDAIA.

REGULATORY FRAMEWORK FOR INTERNATIONAL DATA TRANSFERS

Adequacy and Safeguards

SDAIA is mandated to publish a list of jurisdictions providing an "appropriate level of protection." Evaluation criteria include:

- Existence of data protection laws and compensation mechanisms;
- Independent supervisory authorities;
- Compatibility of foreign disclosure laws with the PDPL;
- International obligations and cooperation; and
- Rules on onward transfers.

As of mid-2025, this adequacy list has not yet been published. In the interim, controllers must implement safeguards such as:

- Standard Contractual Clauses (SCCs);

- Binding Corporate Rules (BCRs); and
- Accreditation certificates from licensed entities.

Exemptions

Data transfers to non-adequate jurisdictions may still occur under exemptions, including:

- Intergovernmental transfers for national interests;
- One-off or limited transfers involving non-sensitive data;
- Centralized processing within multinational groups;
- Direct benefits to the data subject; and
- Scientific research under strict conditions.

These exemptions require robust safeguards and enable data subjects to seek redress for violations.

Subsequent Transfers and Revocation of Exemptions

Transferred data remains subject to the PDPL, even in subsequent transfers. Exemptions may be revoked if safeguards are inadequate, requiring controllers to cease processing and notify recipients.

RISK ASSESSMENT REQUIREMENTS PRIOR TO CROSS-BORDER TRANSFERS

Prior to cross-border transfers, especially for sensitive data or continuous transfers—a risk assessment must be conducted, covering:

- Purpose and legal basis for transfer;
- Data processing scope and geography;
- Safeguards in place;
- Minimization practices and risk controls; and
- Likelihood and impact of harm to data subjects.

Guidelines issued by SDAIA assist in this evaluation.

PRACTICAL RECOMMENDATIONS FOR COMPANIES HANDLING CROSS-BORDER DATA TRANSFERS

To ensure compliance with the Saudi PDPL and related regulations when transferring personal data outside Saudi Arabia, companies should consider the following practical steps:

1. Conduct Data Transfer Mapping and Inventory

- Identify all personal data flows crossing Saudi borders, including types of data, recipients, and jurisdictions.
- Categorize data by sensitivity and volume to assess potential risks and compliance needs.

2. Perform Risk Assessments Prior to Transfers

- Evaluate legal, technical, and operational risks associated with each transfer.
- Consider the data protection standards of recipient countries and any applicable exemptions under PDPL.

3. Implement Adequate Safeguards

- Utilize mechanisms such as SCCs, BCRs, or other safeguards approved or recommended by SDAIA.
- Ensure contracts with third parties explicitly include data protection obligations aligned with PDPL requirements.

4. Determine Whether SDAIA Registration Is Required

- Refer to the SDAIA registration criteria and decision tree to assess the necessity for formal registration of cross-border data transfers.
- Register timely when required to avoid penalties and operational disruptions.

5. Establish Internal Policies and Procedures

- Develop or update data protection policies to reflect PDPL requirements, including cross-border data handling and incident response.
- Train relevant personnel on data transfer compliance and documentation practices.

6. Monitor and Review Compliance Regularly

- Conduct periodic audits and reviews of cross-border data transfers and associated controls.
- Stay updated with any changes in SDAIA regulations, adequacy lists, and enforcement guidelines.

7. Collaborate with Regulators and Industry Peers

- Engage proactively with SDAIA and other relevant authorities to clarify obligations and best practices.
- Participate in industry forums or working groups focused on data protection and cross-border data governance.

8. Document Everything

- Maintain detailed records of transfer decisions, risk assessments, safeguards applied, consents obtained, and registrations made with SDAIA.
- Documentation will support compliance verification and demonstrate accountability.

By following these recommendations, companies can reduce legal risks, protect data subject rights, and align their operations with Saudi Arabia's evolving data protection landscape.

CONCLUSION

Saudi Arabia's updated PDPL marks a significant advancement in its digital transformation strategy. By aligning data governance with cybersecurity, establishing cross-border transfer mechanisms, and reinforcing regulatory compliance through institutions like SDAIA and SAMA, the Kingdom is positioning itself as a regional and global leader in the digital economy.
Organizations operating in Saudi Arabia must now undertake rigorous compliance efforts to meet the PDPL's requirements.

***

POINTS OF CONTACT:

Wissam Hachem
Partner
Wissam.hachem@blkpartners.com

Hala Alsudairy
Junior Associate
Hala.alsudairy@blkpartners.com

This article can also be accessed at: **www.blkpartners.com**