GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

COMMENTS ON PROPOSED AMENDMENTS TO IMPLEMENTING REGULATIONS UNDER THE PERSONAL DATA PROTECTION LAW

SUBMITTED TO THE SAUDI DATA & ARTIFICIAL INTELLIGENCE AUTHORITY (SDAIA)

NOVEMBER 2026

The Global Data Alliance (GDA) welcomes the opportunity to comment on SDAIA's proposed amendments to the Implementing Regulation of the Personal Data Protection Law (PDPL). The GDA is a cross-industry coalition committed to high standards of data responsibility and to the ability to transfer data securely across borders. We support the Kingdom's Vision 2030 objectives, its efforts to strengthen privacy protections, and its ambition to develop a trusted, innovative digital economy. Our comments focus on provisions with particular implications for cross-border data flows and internationally integrated business operations.

1. Avoid a General Personal Data Storage Mandate

Proposed Article 23(2) would require that "The Controller shall store Personal Data within the Kingdom," while continuing to allow transfers or disclosures abroad in accordance with the PDPL and its Implementing Regulations.

Unlike the current regulation, this would establish a general domestic-storage duty, apparently even where a cross-border transfer is otherwise lawful under PDPL Article 29 and the transfer regulations. The draft does not explain whether the primary dataset, a duplicate copy, backups, or all of these must remain in the Kingdom; nor does it define the obligation's application to cloud services or data processed by overseas affiliates and providers.

A blanket location requirement should not be presumed to improve privacy or cybersecurity. Article 23(1) already requires appropriate security safeguards and compliance with applicable National Cybersecurity Authority requirements or recognized standards. These outcome-based obligations can protect Saudi data irrespective of the location of particular servers. By contrast, mandatory local copies can multiply datasets and access points; restrict multi-region resilience and disaster recovery; and require costly changes to globally integrated cloud, analytics, fraud prevention, logistics, manufacturing, health, and financial systems. Saudi organizations and smaller businesses, as well as international investors, would bear these burdens.

GDA recommends that SDAIA **delete proposed Article 23(2)** and continue to rely on a risk-based, accountability-oriented framework that enables lawful transfers using recognized safeguards, including relevant adequacy arrangements, standard contractual clauses (SCCs), and binding corporate rules (BCRs). This would maintain meaningful protection for personal data while avoiding a parallel storage condition that could negate the practical utility of lawful transfer mechanisms.

If SDAIA nonetheless considers a targeted storage measure necessary, GDA recommends limiting it to precisely defined categories of exceptionally sensitive data (e.g., military and defense-related data) for which a specific, demonstrable risk cannot be addressed through less restrictive safeguards. The rule should identify its legal and policy rationale, covered datasets, scope, exceptions, and mechanism for obtaining relief; avoid extending any targeted measure to routine, low-risk business processing where identified risks can be effectively addressed through less restrictive safeguards; and be coordinated with any existing sector-specific requirements to prevent overlap or contradiction.

2. Preserve Workable Cross-Border Transfers and Clarify Technical Scope

SDAIA should expressly confirm that lawful foreign hosting, processing and remote access remain possible under the PDPL transfer framework, and explain how that permission operates. Technical standards should remain technology-neutral and permit effective encryption, access controls, contractual protections, auditability and timely production of information to SDAIA as proportionate measures to meet core data security and data protection goals.

SDAIA should also confirm that Article 23(2) does not prohibit or restrict offshore backup, cross-region replication, disaster recovery, cybersecurity monitoring, incident response, or other resilience arrangements where the relevant transfer or disclosure complies with the PDPL and its Implementing Regulations. Personal Data lawfully transferred outside the Kingdom should be permitted to remain stored outside the Kingdom for the authorized purpose and applicable retention period, subject to the required safeguards, accountability, and regulatory-access obligations.

These questions are consequential for routine systems in cloud-enabled environments in virtually every sector, including employee and payroll platforms, customer relationship management, medical device operation, pharmacovigilance, financial transactions, and international supply chain coordination. A requirement to rebuild such systems solely on the basis of data location risks disrupting services without commensurate improvement in protection. The GDA raised related questions in its April and August 2024 submissions to SDAIA, and encourages clear, internationally interoperable treatment of cross-border data transfers.

In the health and insurance sectors, these arrangements may support continuity of eligibility verification, claims authorization, provider coordination, case management, and other critical services during operational disruption.

3. Revise DPIA Requirements

The proposed amendments to Article 25 would significantly expand the circumstances requiring data protection impact assessments (DPIAs), without adequately distinguishing between routine processing activities and those presenting material risks to data subjects. In particular, Article 25(1)(b) would require DPIAs whenever controllers collect, compare, or link personal data from different sources—a routine feature of enterprise operations, including human resources, customer management, and cloud services—and should therefore be removed or narrowed to higher-risk circumstances. Similarly, Article 25(1)(c) should clarify the meaning of "large scale" and exclude routine monitoring undertaken for cybersecurity, fraud prevention, and other legitimate security purposes, while Article 25(1)(e) should apply only to automated decisions that produce legal or similarly significant effects on individuals. Article 25(1)(a) should also clarify the meaning of "individuals with partial or no legal capacity," as controllers may not reasonably be able to identify all individuals falling within this category. Finally, Article 25(3) should eliminate the blanket requirement to provide processors with copies of DPIAs, which would impose significant administrative burdens and potentially require disclosure of confidential commercial, operational, and security information.

4. Narrow the Cross-Border Registration Trigger

Proposed Article 34(1)(d) would require a controller to register with the National Register of Controllers whenever it transfers personal data outside the Kingdom or discloses it to an overseas entity. As drafted, this criterion would reach routine and low-risk activity across multinational groups and domestic businesses using offshore services, regardless of the nature or scale of processing. It could generate extensive low-value filings for both controllers and SDAIA, although Article 33 already provides for regulatory access to records of processing activities.

GDA recommends deleting Article 34(1)(d), or alternatively limiting registration to objectively defined, high-risk cross-border processing. If Article 34(1)(d) is retained, SDAIA should expressly clarify that registration is an administrative transparency obligation – not a condition for a transfer that is otherwise lawful under the PDPL. Registration should occur at the controller level, or on a consolidated group basis where appropriate, and should not require a separate filing for each transfer, disclosure, recipient, or recurring operational data flow.

5. Transition and Continued Consultation

Proposed Article 38 provides for entry into force 60 days after publication in the Official Gazette. Where a final measure requires material changes to hosting architecture, resilience arrangements, contracts, vendor configurations, or data-governance controls, SDAIA should provide a phased transition period commensurate with those changes, together with appropriate treatment for existing deployments and timely technical guidance. Many of the proposed changes in the Implementing Regulations will upend the PDPL norms upon which international businesses have structured their investments for years. For these changes, **a minimum 24-month period** would be required.

6. Retain a Risk-Based Breach Notification Threshold

Proposed Article 24 would remove the harm threshold for notifying SDAIA of a personal data breach, so that even low-risk incidents could require notification within 72 hours. This would generate a high volume of low-value

notifications and divert controller and SDAIA resources from incidents that pose genuine risk to Data Subjects. GDA recommends that SDAIA retain a risk-based notification threshold, in line with international practice.

6. Recognize role of corporate group DPOs in a cross-border context

While the GDA supports institutionalizing privacy leadership, the regulation lacks explicit flexibility for multi-jurisdictional enterprises. In globally integrated sectors (e.g., banking, cloud technology, aviation), organizations typically rely on regional or cluster DPO models where seasoned privacy officers oversee multiple entities, supported by local teams. Mandating separate, in-Kingdom DPOs for every legal entity would create severe resource constraints given the market scarcity of certified privacy professionals, without improving compliance outcomes. We urge SDAIA to clarify that corporate groups may appoint a single Group or Regional/Cluster DPO across affiliated entities in the Kingdom, provided the officer is easily accessible to SDAIA and data subjects and understands local regulatory requirements. We also ask that SDAIA clarify that Article 32(1) does not mandate domestic physical residency for internal or external DPOs, provided effective communication channels, timely response protocols, and designated local liaisons are maintained.

7. Conclusion

GDA appreciates SDAIA's engagement with stakeholders and would welcome further dialogue on approaches that advance privacy, security, regulatory oversight and Saudi Arabia's digital economy objectives without unnecessarily restricting trusted cross-border data flows. If you have any questions, please feel free to contact Joseph Whitlock, Executive Director, Global Data Alliance, at jwhitlock@bsa.org.