SDAIA · PDPL · REGULATORY BRIEFING · Regulatory Briefing · July 2026

Cross-border data transfer under PDPL: an operational checklist

By Oxon Research

For international organizations operating in Saudi Arabia, no PDPL topic generates more day-to-day friction than cross-border transfers. Group IT runs on regional cloud infrastructure, HR and CRM systems sit at headquarters abroad, support teams work follow-the-sun — and every one of those arrangements moves personal data outside the Kingdom. Since the Regulation on Personal Data Transfer Outside the Kingdom entered into force in September 2024, and with SDAIA's enforcement now fully operational, “we'll formalize it later” is no longer a position a controller can defend.

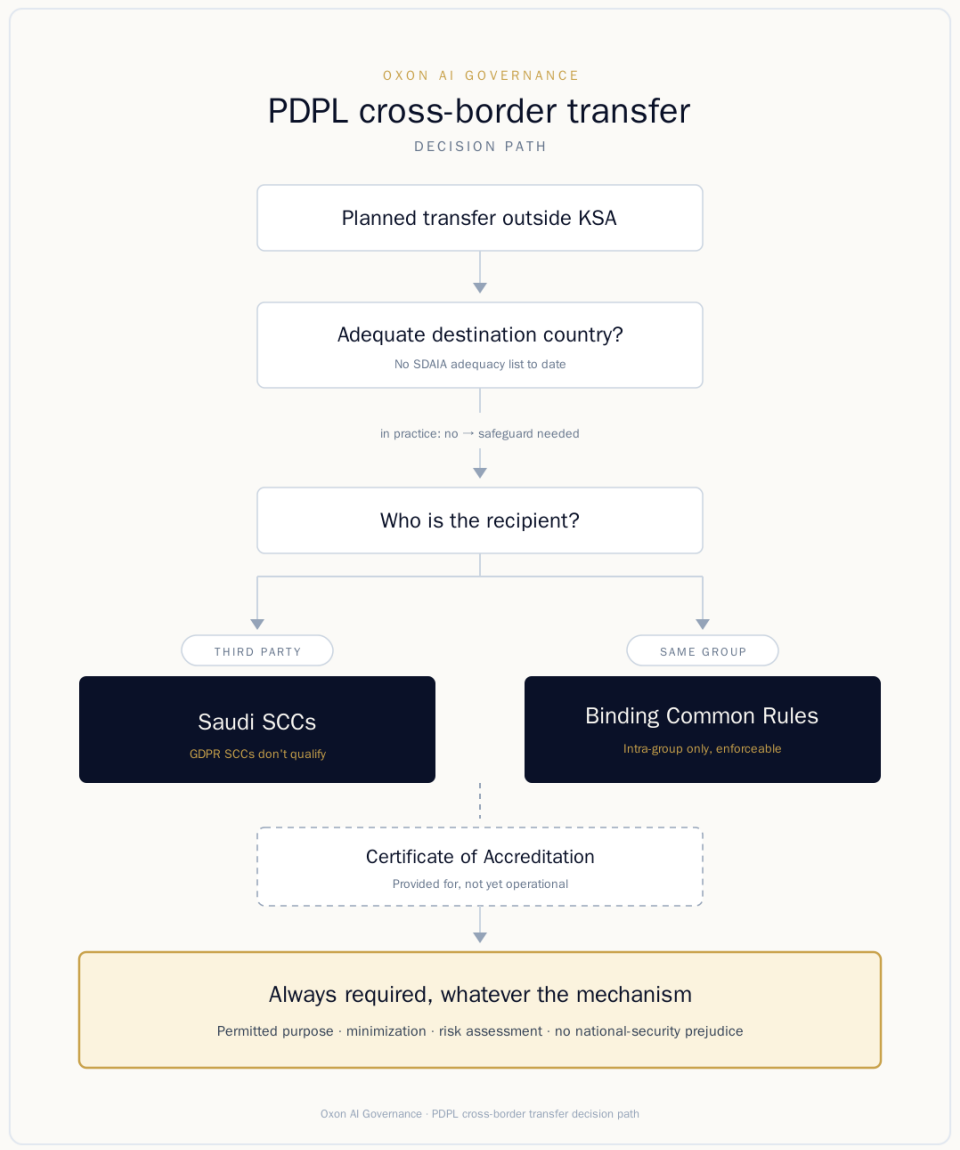
This briefing sets out the questions a Saudi controller must be able to answer — and the evidence behind each answer — before data leaves the Kingdom.

The structure of the regime, in one paragraph

PDPL's starting point (Article 29) is that transfers outside the Kingdom are restricted unless conditions are met. The Transfer Regulations then build a layered system: the transfer must serve a permitted purpose; it must rest on an adequacy determination or an appropriate safeguard — Saudi Standard Contractual Clauses, Binding Common Rules for intra-group transfers, or a Certificate of Accreditation; it must be limited to the minimum data necessary; it must not prejudice national security or the Kingdom's vital interests; and, for higher-risk transfers, it must be preceded by a documented risk assessment. Each layer is a separate obligation, and each generates its own evidence requirement.

The operational checklist

Choosing the mechanism — the short version. Before working through the checklist, one decision drives everything else: which transfer mechanism applies. In practice the path is short. Adequacy would be the simplest route, but with no adequacy list published by SDAIA to date, it is not available in practice. That leaves the appropriate safeguards, and the choice between them turns on who the recipient is: for transfers to third parties (vendors, cloud providers, partners), Saudi SCCs are the working answer — noting that GDPR SCCs do not satisfy the Saudi requirement; for intra-group flows, Binding Common Rules can cover the whole group, provided they are legally binding on every entity and enforceable by data subjects. The Certificate of Accreditation exists in the texts but is not yet operational as a primary basis. And whichever mechanism applies, it is only one layer: permitted purpose, minimization, risk assessment where required, and the national-security condition apply in every case.



01 Do you actually know your transfers? Map every flow of personal data out of the Kingdom — including the ones that don't look like transfers: remote access by an offshore support team, group-wide HR dashboards, cloud backups replicated across regions, analytics SDKs in customer-facing apps. Under the PDPL, disclosure to another legal entity is a transfer even within the same corporate group.

Evidence — a transfer inventory, kept current, reconciled with your records of processing.

02 Is each transfer tied to a permitted purpose? The Transfer Regulations enumerate the purposes for which transfer is allowed — including performing contractual obligations and processing operations that enable the controller to carry out its activities, such as central management functions. Generic convenience is not a purpose.

Evidence — the purpose recorded per transfer, in language that matches the Regulations, not internal shorthand.

03 What is your transfer mechanism — and can you produce it? With no adequacy list published by SDAIA to date, in practice most transfers rest on an appropriate safeguard. For third-party transfers, that generally means Saudi SCCs — note that GDPR SCCs do not satisfy

the Saudi requirement; the clauses must reflect PDPL obligations and data subject rights, including compensation. For intra-group flows, Binding Common Rules can cover the group, but they must be legally binding on every entity and enforceable by data subjects — an internal policy PDF does not qualify.

Evidence — executed clauses or approved BCRs, retrievable per transfer, not "somewhere in legal."

04 Have you done the risk assessment — and does it cover the five required elements? For transfers involving sensitive data on a continuous or large-scale basis, a risk assessment is mandatory, and SDAIA published a dedicated guideline for it in February 2025. Under Article 7 of the Transfer Regulations, the assessment must address: the purpose of the transfer; the nature and geographical scope of the processing; the safeguards implemented; the adequacy of the recipient's protection relative to PDPL; and the minimization measures applied. An assessment missing any element is a gap, not a formality.

Evidence — the assessment document itself, dated before the transfer began.

05 Is the data minimized — demonstrably? "Minimum necessary" is a substantive test the controller must be able to defend field by field: why does the offshore CRM need national ID numbers? Why does the analytics pipeline receive full birth dates rather than age bands?

Evidence — a data-field justification for recurring transfers, reviewed when systems change.

06 Have you reconciled PDPL with your sector's rules? PDPL is the general regime, not the only one. Financial institutions face SAMA's expectations, including no-objection requirements for certain outsourcing and data arrangements; organizations in scope of the National Cybersecurity Authority must align transfer security with the Essential Cybersecurity Controls, whose data residency logic can be stricter than PDPL's. Where regimes overlap, the stricter control governs.

Evidence — a per-sector mapping showing which requirement prevails for each transfer — this is where most programs we review have their largest gap.

07 Could you demonstrate all of this next week? PDPL accountability means demonstration on request: controller registration in order, transfer documentation retrievable, DPO appointed where required — noting that conducting cross-border transfers is itself one of the triggers for mandatory DPO appointment. Administrative fines reach SAR 5 million and can double for repeat violations; SDAIA's enforcement committees have been issuing decisions since 2025.

Evidence — a dry run. If assembling your transfer file takes more than a few days, it will not survive a real request.

The bottom line

Cross-border compliance under PDPL is not one decision but a chain of them — purpose, mechanism, assessment, minimization, sector reconciliation — and the chain is only as strong as its weakest documented link. Organizations that treat the Transfer Regulations as a contracting exercise ("sign the SCCs and move on") consistently fail at steps 1, 4 and 6. Organizations that treat them as an evidence exercise pass audits, close enterprise deals faster, and answer SDAIA in days rather than weeks.

Oxon X helps organizations evidence lawful transfers and reconcile PDPL with sector-specific controls.

Schedule a compliance audit → contact@oxonx.sa