TEMAIRIK

LAW

EXECUTIVE BRIEFING 2026

Saudi Personal Data Overseas Access, Transfers & Vendor Risk

Five decisions management should resolve before Saudi personal data becomes accessible outside the Kingdom.

TEMAIRIK

LAW / SAUDI ARABIA

THE MANAGEMENT DECISION

Hosting location is not the end of the transfer analysis.

An overseas server is not the only way Saudi personal data can cross a border. Remote access by a group company, support team, cloud provider or other recipient outside the Kingdom can be part of the analysis even where the primary system remains hosted in Saudi Arabia.

THE FIVE QUESTIONS

- What personal data will be transferred or accessible?
- Why is the overseas access necessary and on what basis?
- Which Saudi transfer route applies?
- Which contractual, technical and organisational safeguards are in place?
- Has every required assessment been completed before access begins?

OPERATING PRINCIPLE

The legal work should begin with the live architecture - not the title of the contract or the location printed on an invoice. The contract, data map and live system configuration should tell the same story.

01 / MAP THE LIVE ARRANGEMENT

Describe the transfer precisely.

Labels such as employee data, customer data or cloud access are not a sufficient map. Counsel needs the live facts that determine the transfer route, risk and safeguards.

DATA

What is involved?

Data fields, sensitive-data status, data subjects, purpose, legal basis, retention and deletion.

ACTORS

Who can act?

Saudi controller, processors, sub-processors, group recipients, support teams and accountable owners.

LOCATIONS

Where can access occur?

Storage, backup, support and administration countries, plus any onward recipient or transfer route.

SYSTEMS

How does it happen?

Applications, interfaces, identity controls, download rights, logging, support tooling and technical restrictions.

EVIDENCE TO RECONCILE

- Architecture and data-flow diagrams
- Vendor and sub-processor schedules
- Identity and access settings
- Processing records, notices and retention schedules
- Contracts, transfer safeguards and risk assessments

02 / SELECT THE ROUTE AND SAFEGUARDS

The route follows the facts.

There is no responsible single answer for every destination, recipient or intra-group arrangement. The controller should document the route for each material flow and the conditions on which that route depends.

01 **Purpose & basis**

Define the commercial or legal purpose, identify the relevant recipient and limit the data to what that purpose requires.

02 **Transfer route**

Assess the source, destination, recipient, level of protection, any appropriate safeguard, any limited exception and relevant sector restriction.

03 **Safeguards**

Where the appropriate-safeguards framework applies, SDAIA materials identify standard contractual clauses, binding common rules and accreditation certificates.

04 **Risk assessment**

Complete the required assessment before access where the Transfer Regulation requires it, and turn its controls into conditions for approval.

03 / ALIGN THE DOCUMENTS AND THE SYSTEM

A data-processing agreement is evidence of analysis. It is not the analysis.

A well-drafted processing agreement can allocate instructions, confidentiality, security, sub-processing, incident reporting, audit support and deletion. It does not, by itself, determine the Saudi transfer route or prove that the technical architecture follows the agreed restrictions.

REQUIRED ALIGNMENT

- Approved purpose and minimum data set
- Selected transfer route and executed safeguard
- Risk-assessment controls and accountable owner
- Role-based access, authentication, logging and monitoring
- Incident route, onward-transfer controls and deletion
- Notices, processing records and review triggers

DECISION RECORD

For each material flow, retain the current map, purpose and basis, parties and destinations, selected route, safeguard, required assessment, technical-control evidence, approvals, responsible owners, review date and change triggers.

TEMAIRIK LAW

Saudi Data, Technology & Brand Readiness Review

A fixed-scope legal assessment connecting Saudi data protection, technology and cloud arrangements, cybersecurity responsibilities, brand and intellectual-property protection, and the business dependencies that materially affect the reviewed activity.

- Executive issue map
- Focused evidence request
- Risk-ranked 90-day priorities
- Scoped implementation proposal

Request the review
temairiklaw.sa/en/services/data-technology-brand-readiness/

OFFICIAL SAUDI MATERIALS

Transfer Regulation
https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/RegulationonPersonalDataTransferOutsidetheKingdom/

Transfer Risk Assessment Guideline
https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/RiskAssessmentGuideline%20orTransferringPersonalData/

Standard Contractual Clauses
https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/StandardContractualClauses/

Binding Common Rules Guidance
https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/GuidelinesforBindingCommonRules/