



ASTRAGAR

DON'T BE VULNERABLE

SAUDI PERSONAL DATA PROTECTION LAW

Enforcement arrived 48 decisions ago.

None of them needed a breach. A briefing on what SDAIA actually penalised, the transfer route that does not exist yet, and what the gap is worth — for security, privacy and legal leaders in the Kingdom.

48

Violation decisions,
year to 16 Jan 2026

72 HOURS

To notify SDAIA, from
becoming aware

SAR 5M

Per violation. Doubled
for repeat offences

What SDAIA actually penalised

On 16 January 2026 SDAIA confirmed that its Committees for Reviewing Violations had issued **48 decisions confirming violations** over the preceding year, and applied the penalties prescribed by the law. The conduct fell into four categories.

- Collecting and processing personal data **without a legal basis**
- Disclosing personal data **without legal justification**
- Failing to implement adequate **organisational, administrative and technical safeguards**
- Sending **marketing messages without consent**

Not one of those requires a security incident. No attacker, no exfiltration, no data loss. Every one is a finding available to an auditor reading your documentation.

Most organisations in the Kingdom are preparing for a breach. The decisions are coming from the paperwork.

Forty-eight decisions in a year is not a large number by European standards, and it would be a mistake to read it as a crackdown. It is better read as a signal of **what the committees look at first** — and the answer is governance artefacts, not forensics.

WHO IS IN SCOPE

Including entities outside the Kingdom

PDPL applies to any processing of personal data relating to individuals residing in Saudi Arabia, by any entity, **including entities located outside it**. There is no establishment test and no targeting test. Foreign parents holding KSA employee data, offshore shared-service operations and SaaS providers storing KSA data in another region are all caught.

There is still no adequacy list.

PDPL permits transfers to a jurisdiction SDAIA determines has an adequate level of protection. SDAIA has not published which jurisdictions those are — so the route the regulation offers you has not been built yet.



Every transfer runs on a safeguard

With no adequacy route available, a transfer out of the Kingdom must satisfy a permitted purpose and then rest on one of three appropriate safeguards.

SAFEGUARD 01

Saudi standard contractual clauses

Issued in modular form: controller-to-controller, controller-to-processor, processor-to-processor and processor-to-controller.

SAFEGUARD 02

Binding common rules

Available for intra-group transfers only.

SAFEGUARD 03

Certificate of accreditation

Issued by an approved body.

And a risk assessment before the data moves

SDAIA's February 2025 guideline makes a documented risk assessment mandatory for any transfer using appropriate safeguards. It must evaluate:

- 1 The purpose and nature of the transfer
- 2 The geographic scope of the processing activities
- 3 The safeguards and protective measures implemented
- 4 The adequacy of the recipient
- 5 Data minimisation measures applied

Suitability of the chosen safeguard is reviewed **every two years**.

Why this is the largest exposure we find

- **Transfers are architectural.** They are made by a cloud region setting, a group IT consolidation or an outsourcing contract — decisions taken years before anyone wrote a data map.
- **They are continuous.** An undocumented transfer is not a historic event that has passed; it is happening every day until someone papers it.
- **They are documentary by nature,** which puts them squarely in the category of conduct the committees have shown they penalise.

The 72-hour clock

72h

Notify SDAIA

Through the National Data Governance Platform, from becoming aware.

ASAP

Notify individuals

Affected data subjects, without undue delay.

0

Submission APIs

Nothing files automatically out of your existing tooling.

The platform does not record when you became aware. You evidence that timestamp yourself, from your own logs, tickets and escalation trail.

So the question is not whether you can file inside 72 hours. It is whether you can prove, afterwards and to a third party, **when the 72 hours started**. Those are different problems, and only one of them is usually solved.

In most organisations the awareness moment is distributed across a SIEM alert, a service-desk ticket, a chat thread and somebody's recollection. That is not evidence.

Cloud service providers may carry additional reporting obligations to the Communications, Space and Technology Commission.

Registration is not a formality

Registration on the National Data Governance Platform is mandatory for:

- All **public entities**
- Any controller whose **core activity involves processing personal data**
- Any controller processing **sensitive personal data** at all

No derogation for small organisations. Certificates run five years. The same platform holds your DPO's appointment details and receives your breach notifications.

A DPO must be appointed where a public entity processes at large scale while providing services, where core activities involve regular and systematic monitoring of data subjects, or where core activities involve sensitive data. The DPO must be academically qualified with demonstrable expertise.

WHAT THE HIRING DATA SHOWS

Across the Kingdom, senior privacy and data-protection roles remain thin on the ground relative to the number of organisations that now need one. Where the role is unfilled, the registration record shows it — and that is the first thing an audit reads.

Penalties

BREACH	MAXIMUM	NOTES
Administrative violations	SAR 5,000,000	Per violation. Warning or fine. Courts may double for repeat offences.
Unlawfully disclosing sensitive personal data with intent to harm or for personal benefit	SAR 3,000,000	And/or up to 2 years imprisonment.
Unauthorised cross-border transfer	SAR 5,000,000	Attracts the administrative penalties.

Additional remedies include confiscation of proceeds and publication of the judgment at the violator's expense. For a regulated institution the publication remedy is frequently the more expensive half.

Twelve questions

If you cannot answer any one of them in a sentence, that is where to start.

- 1 Who registered this organisation on the National Data Governance Platform, on what date, and against what description of our processing?
- 2 Are we required to appoint a DPO, and if so is the appointment filed?
- 3 Can we produce a processing register that names a lawful basis **per purpose**, not per system?
- 4 Where consent is our basis, was it obtained separately for each purpose, and can we evidence it?
- 5 List every flow of personal data outside the Kingdom. Does the list come from architecture or from memory?
- 6 For each of those flows, which appropriate safeguard does it rest on?
- 7 For each flow, does a documented risk assessment exist, dated before the transfer began?
- 8 When was each safeguard last reviewed, and when is the two-year review due?
- 9 If we detected a breach this afternoon, who files, through what credential, and by when?
- 10 Could we prove to a third party when we became aware of it?
- 11 How does a data subject exercise their rights, and what is our actual turnaround, measured?
- 12 If SDAIA asked for our documentation tomorrow, what would we send, and who owns it?

Every item here can be closed. The reason most are not is that the work competes for budget against initiatives that arrive with a number attached — and compliance remediation usually does not.

We supply the missing number.

- Classify your personal data processing against PDPL — basis, registration, DPO position, retention, data subject rights
- Map every transfer out of the Kingdom and the safeguard it relies on, and produce the risk assessments the regulations require
- Test the breach pathway end to end, including whether the awareness timestamp is evidenced
- Price the residual exposure in dollars, using a method an underwriter recognises
- Place the cyber cover behind it, where that makes sense

**The regulation tells you to assess your risk.
We tell you what it costs.**

INTRODUCTORY PRICING

**PDPL readiness from USD 10,000,
for our first five engagements in the
Kingdom.**

A 20-minute scoping call is enough to tell you which of the twelve questions you would struggle with.

astragar.com/use-cases/pdpl

SOURCES

Saudi Personal Data Protection Law, Royal Decree M/19 (2021, as amended 2023), its Implementing Regulations and the Regulations on Personal Data Transfer outside the Kingdom · SDAIA via Saudi Press Agency, 16 January 2026 · SDAIA data transfer risk assessment guideline, February 2025 · DLA Piper, Data Protection Laws of the World · King & Spalding on international transfers.

This pack is information, not legal advice. Confirm your position with a Saudi-qualified adviser.