lemnisk

CDP for Saudi Arabia - PDPL Compliance and Local Data Residency

PDPL fully enforceable

Sep '24

Max fine per violation (doubled for repeat)

$1.3M

Mandatory data processing records retention

5 yrs

What is the PDPL?

Saudi Arabia's first comprehensive Personal Data Protection Law (PDPL) issued by Royal Decree and enforced by SDAIA. Applies to any entity inside or outside the Kingdom that processes the personal data of Saudi residents.

Why it matters for CDPs

A CDP is the central repository for customer PII - behavioral, transactional, demographic. Every collect, store, activate, and export action is in scope. Default SaaS CDP architectures are non-compliant by design.

4 PDPL obligations every CDP must address

Lawful basis & consent	Consent is the default. CDP must capture, store, and honour consent signals and support withdrawal in real time.
Data subject rights	Right to access, correct, and delete personal data. CDP must enable rights fulfilment across all unified profiles.
DPO & governance	Appoint a Data Protection Officer. Maintain a Record of Processing Activities (ROPA) for 5 years post-activity.
Cross-border transfers	Only to adequate jurisdictions or via SDAIA-approved SCCs/BCRs. EU SCCs alone are insufficient.

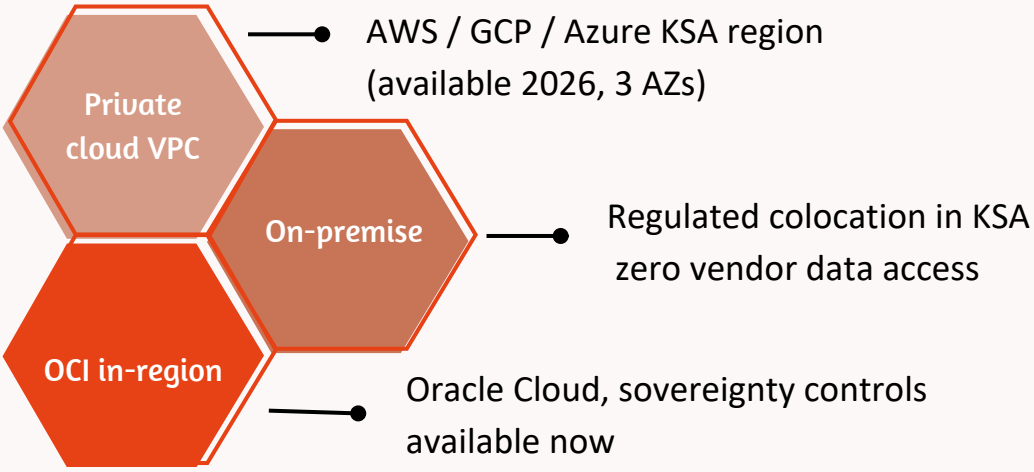
Data residency requirement

Personal data of KSA residents must be stored and processed within the Kingdom. This extends to backups, replicas, and snapshots not just primary databases. Cloud Computing Regulations (CCSPRs) reinforce this for public-sector data.

Why SaaS CDPs fail

- Data replicated to foreign nodes by default
- Disaster recovery fails over outside KSA
- Vendor support teams access data offshore
- No in-country deployment option
- EU SCCs used — not SDAIA-approved

Compliant CDP deployment options in KSA



PDPL Readiness - Quick Checklist

- [ ] Data fully stored and processed within KSA
- [ ] Consent lifecycle (capture → withdrawal) enforced in real time
- [ ] Data subject rights handled across unified profiles
- [ ] Cross-border transfers aligned with SDAIA-approved mechanisms
- [ ] Clear DPO ownership + ROPA retention (5 years)
- [ ] Full audit trail + restricted in-country access

Ready for a PDPL-compliant CDP?

See how Lemnisk enables real-time customer engagement with full data residency and consent control in Saudi Arabia. **Get a Demo**