

PDPL

Critical Needs for Businesses
to Comply with PDPL

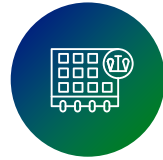
Personal Data Protection Law



Saudi Arabia's Personal Data Protection Law (Royal Decree M/19 of 17 Sept 2021) governs the processing of personal data within the Kingdom.



It applies to all organizations, including public agencies, state-owned enterprises, listed companies, SMEs, and foreign groups.

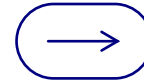


The law came into effect on 14 September 2023.



A one-year grace period ended on 14 September 2024, making full compliance mandatory as of today.

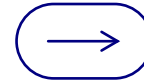
Consequences of Non-Compliance



Non-compliance can trigger fines up to **SAR 5 million** (doubled for repeat offences) and, for wilful disclosure of sensitive data, up to two years' imprisonment!!













SDAIA's Audit and Inspection Enforcement



SDAIA already conducts ad-hoc audits and public-sector inspections and has **warned that penalties—and public naming**—will follow for entities that cannot demonstrate real, operating privacy governance.



Who must comply with Saudi Arabia's Personal Data Protection Law (PDPL)?

 Sector	Typical in-scope Saudi players
 Government & state-owned	Ministries, municipalities, courts, police forces; national champions such as Saudi Aramco, SABIC, Ma'aden, Saudi Railways
 Financial services	All licensed banks (SAMA), insurers, fintechs, payment networks & credit bureaus
 Telecom & ICT	Telecom, data-centre and cloud providers, ISPs
 Healthcare	Public & private hospitals, clinics, lab chains, health-tech platforms
 Retail & e-commerce	Brick-and-mortar giants (e.g., Panda, Bin Dawood), online marketplaces, loyalty-card operators
 Hospitality & travel	Airlines, hotels, GIGA-project resorts, online booking engines
 Education	Universities, schools, EdTech platforms processing student data
 Utilities & critical infrastructure	Water, power, oil & gas distribution, smart-city OT operators
 SMEs & start-ups	Any LLC or start-up that stores HR, customer or supplier data—even a 5-person SaaS firm



Saudi Arabia's most-publicized data breaches in 2025 & 2024 — and what they are likely to have cost

Year	Victim (sector)	What happened	Size / ransom demand	Indicative financial impact*
2025	Al Bawani – Riyadh-based design-build contractor (construction & real-estate)	DragonForce ransomware used dual-extortion tactics; > 6 TB of project drawings, air-base plans and bid documents dumped after the deadline passed	No figure published; comparable DragonForce leaks this size have carried US \$8–12 m opening demands	≈ US \$6–8 m (SAR 23–30 m) for recovery, legal, stalled tenders and delayed mega-projects Built Environment MagazineDark Reading
	Royal Saudi Air Force (defence)	KillSec posted encrypted RSF email archives and logistics spreadsheets on its leak site	Records volume not disclosed	Highly sensitive; IBM puts public-sector breaches in ME at ≈ US \$7-9 m on average
	General-Intelligence/MoD internal centre (government)	Babuk2 listed the target on 3 Apr 2025; files advertised included personnel lists and budget sheets	Undisclosed	Similar government intrusions historically cost US \$6-9 m once IR, clean-up and OT separation are included
	Rawafid Industrial (critical water infrastructure)	Ralord ransomware, discovered 23 Apr 2025; threatens OT diagrams & SCADA configs	Undisclosed	OT outages + emergency consulting typically push losses above US \$5 m
2024	Saudi Government portal (saudi.gov.sa)	Pryx offered an entire CMS dump on a dark-web forum (27 Aug 2024)	Leak size “unknown”	Expected to trigger PDPL-notification costs and re-platforming—≈ US \$5-6 m
	Oxyhealth Clinics (private healthcare)	“Kill” group exfiltrated PII & electronic health records; ransom deadline 18 Nov 2024	Volumes not stated	Healthcare is the most expensive vertical; likely US \$7-10 m (SAR 26-37 m) in direct + litigation costs



What this means for Saudi organizations in 2025?



Construction and real estate are now high-value targets— Digital twins, BIM files and giga-project blueprints give attackers leverage even when personal data volume is low.



Public-sector and defence leaks carry disproportionate downstream costs (national-security investigations, contracts re-tendered).



Healthcare remains the costliest vertical because PDPL, potential SDAIA sanctions and class-action exposure stack on top of ransomware extortion.



Average breach cost is accelerating faster in the Middle East (+10 % YoY) than globally (+7 %), driven by faster adoption of SaaS and smart-city OT.



Broader 2024-25 landscape



88 Saudi ransomware cases in 2024— manufacturing (25 %), information services (11 %) and construction (10 %) were the top targets, according to SOCRadar's threat-landscape report **SOCRadar® Cyber Intelligence Inc..**










Average record-level cost in the Middle East hit **US \$188 per record**, IBM/Ponemon data show, pushing mega-breach (≥ 1 M records) exposure toward the US **\$35-60 m** zone for outlier events



Regulatory pressure is rising: SDAIA's October 2024 breach-notification guide enforces a 72-hour window and fines that now exceed **US \$100 k** in 1 in 5 Saudi cases



How SDAIA is policing the law

 Mechanism	What it looks like in practice	Legal basis
 Administrative fines & criminal penalties	Routine infringements: warning or fine up to SAR 5 million (≈ US \$1.3 m). Intentional disclosure of sensitive data: prison up to 2 years and/or SAR 3 m. Repeat offences: court may double the fine.	Art. 29 & 30 PDPL; SDAIA enforcement powers DLA Piper Data ProtectionSDAIA
 72-hour data-breach notification	Controllers must alert SDAIA within 72 h of becoming aware of a breach, and inform affected individuals “without undue delay”.	Implementing Regs §36 DLA Piper Data Protection
 On-demand audits & information requests	SDAIA (or later the National Data Management Office) may “request the necessary documents or information from the controller to ensure compliance” and can enter premises or mandate third-party audits.	Implementing Regs Arts 58-60; PDPL Art 26 SDAIASDAIA
 Registration & ongoing supervision	High-risk controllers must register on SDAIA’s PDPL portal, file processing registers, and appoint a locally-based DPO under Rules for Appointing a DPO (Aug 2024).	SDAIA DPO Rules 2024 HFW
 Cross-border-transfer controls	Transfers outside KSA must use SDAIA Standard Contractual Clauses (SCCs) or other approved safeguards; SDAIA can demand copies and audit compliance with the SCCs.	SCC templates §8 (“Importer must cooperate with audits”) SDAIA
 Sector co-regulation & referrals	Banking, telecoms and critical-infrastructure supervisors (SAMA, CST, NCA) continue to enforce their own cybersecurity / privacy rules; SDAIA can refer criminal matters to the Public Prosecution.	PDPL Arts 31-32 SDAIA

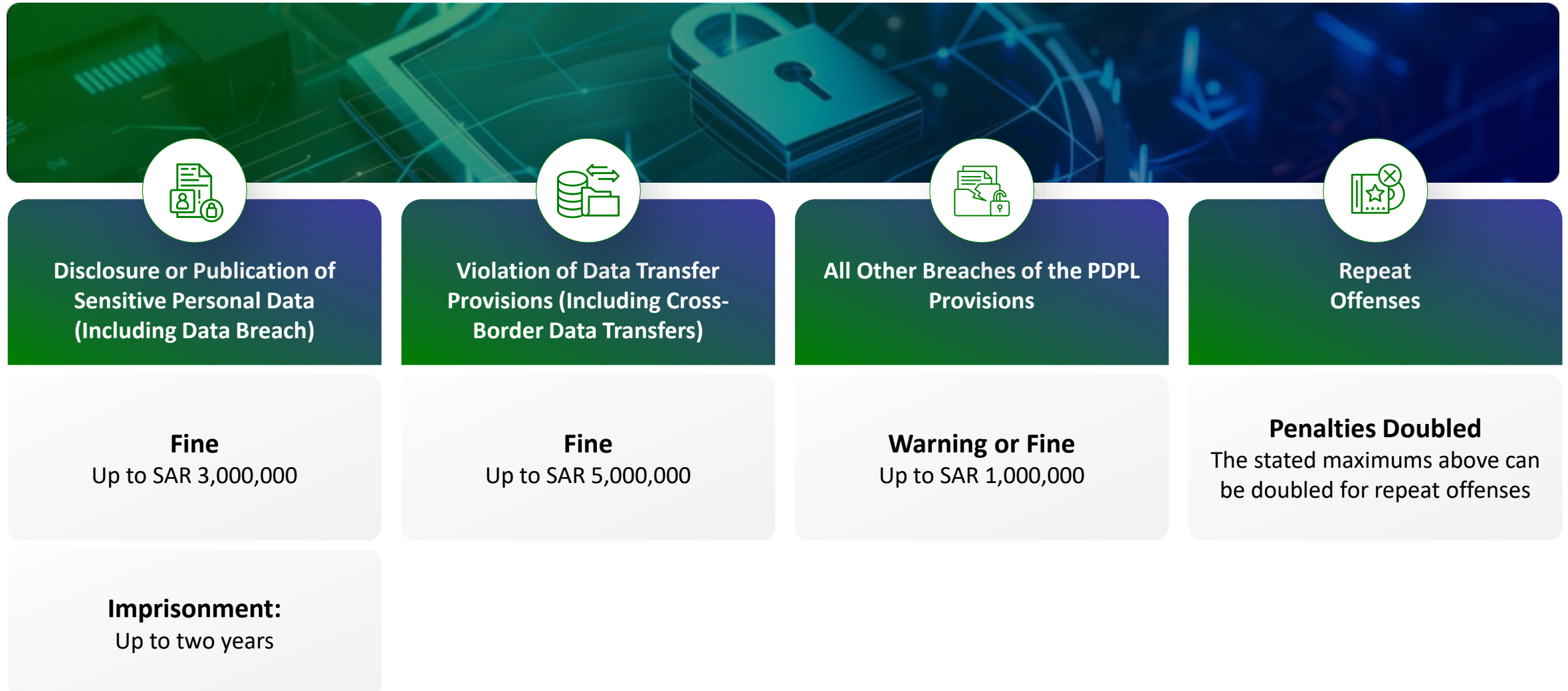




THE CRITICAL NEED FOR COMPANIES TO COMPLY WITH THE PERSONAL DATA PROTECTION LAW (PDPL)

ACT NOW!

PDPL Fines and Penalties



PDPL

Importance, Consequences Call To Action

Protecting Data,
Empowering Businesses

Why is PDPL Important?



Protecting Individual Privacy Rights

Safeguards personal information ethically and legally.



Legal Compliance

Mandatory for all organizations in KSA to avoid penalties.



Building Consumer Trust

Enhances customer confidence in data handling practices.



Aligning with International Standards

Facilitates global business operations and data transfers.



Encouraging Responsible Data Practices

Promotes transparency and accountability.



Supporting Digital Transformation

Aids in achieving KSA's Vision 2030 objectives.



What does PDPL Protect?



Personal Data

Information identifying an individual directly or indirectly.



Sensitive Personal Data

Health, genetic, biometric, religious beliefs, etc.



Data Subject Rights

Access, correction, deletion, objection, data portability.



Data Processing Principles

Lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.



What are the Consequences of Non-Compliance?



Legal Consequences

Severe penalties, fines, and sanctions.



Operational Disruptions

Business interruptions due to data breaches.



Inability to Conduct International Business

Barriers due to data transfer restrictions.



Financial Losses

Direct fines and indirect losses from reputational damage.



Loss of Competitive Advantage

Customers may prefer competitors with better data protection.



Cybersecurity Risks

Higher vulnerability to cyber-attacks.



Reputational Damage

Loss of customer trust and negative publicity.



Regulatory Scrutiny

Increased audits and mandatory oversight.



Employee Morale & Trust

Decreased confidence among staff.



Cost of Data Breach by Industry in Saudi Arabia



Energy Sector
SAR 36.9 M

Reason

Highly interconnected infrastructure, critical operations.



Financial Services
SAR 35.81 M

Reason

Sensitive financial data and strict regulatory demands.



Industrial Sector
SAR 34.52 M

Reason

Involvement of intellectual property and operational technology.



Healthcare Sector
SAR 38 M

Reason

High costs due to sensitive personal health information.



Retail Sector
SAR 32 M

Reason

Large volumes of customer and payment data.







Government Sector
SAR 31 M

Reason

Sensitive citizen data, national security risks.



Cost of Data Breach by Industry in Saudi Arabia

 <p>Technology and Telecommunications</p> <p>SAR 33 M</p>	 <p>Education Sector</p> <p>SAR 29 M</p>	 <p>Hospitality Sector</p> <p>SAR 30 M</p>	 <p>Corporate & General Business Services</p> <p>SAR 28 M</p>	 <p>Real Estate</p> <p>SAR 30.5 M</p>
<p>Reason</p> <p>Extensive personal and operational data.</p>	<p>Reason</p> <p>Student records and research data.</p>	<p>Reason</p> <p>Customer payment information and travel preferences.</p>	<p>Reason</p> <p>Client data, confidential business information, and operational disruptions.</p>	<p>Reason</p> <p>Large datasets on property owners, financial transactions, and regulatory data.</p>




Call to Action!



Contact Us

 AEZ Digital (AEZ LLC, KSA)

 +966 53 271 8855

 faiz@aezdigital.com

“

Data privacy is more than a legal requirement; it's a promise of integrity. In a digital world, the cost of neglecting data protection far outweighs the investment in compliance. PDPL isn't just a regulation—it's a path to building unshakable trust and competitive advantage. Act now and make data protection your strongest asset.