Saudi Arabia's Personal Data Protection Law: A Comprehensive Overview

Type	Legislative Insight
Date	15 Jan 2026
Jurisdiction	Saudi Arabia
Copyright	LexisNexis
Legal reference	Saudi Arabia Cabinet Decision No. 98/1443 Personal Data Protection Law, Saudi Arabia Royal Decree No. M19/1443 On the Approval of the Personal Data Protection Law, Saudi Arabia Administrative Decision No. 1516/1445 Approving the Implementing Regulation of the Personal Data Protection Law

Overview

In recent years, the Kingdom of Saudi Arabia (KSA) has made data protection a central pillar of its legal and economic reforms, reflecting the country's ambition to build a trusted digital economy under its Vision 2030 agenda. At the heart of this transformation is Saudi Arabia Cabinet Decision No. 98/1443 Personal Data Protection Law (Saudi Arabia Royal Decree No. M19/1443 On the Approval of the Personal Data Protection Law), a regulatory framework designed to safeguard personal data, enhance privacy rights, and regulate how both public and private entities handle personal information. The law was originally enacted under Saudi Arabia Royal Decree No. M19/1443 on 15 September 2021 and later amended by Royal Decree No. M/148 on 27 March 2023 coming into force on 14 September 2023, with a phased compliance period extending into 2024.

This enactment is Saudi Arabia's first comprehensive statute regulating governance of the personal data regime. It is applicable to any processing of personal data related to individuals in the Kingdom whether the processing takes place inside Saudi Arabia or involves organisations outside its borders processing the data of Saudi residents. This broad territorial scope is similar to other modern data protection laws and is a key aspect of the law's applicability.

Scope and definitions

One of the most important definitions to consider under Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) is the definition of 'personal data' which essentially means any information that can directly or indirectly identify an individual. This includes names, identification numbers, contact information, financial details, photos, etc. Then comes the meaning of 'sensitive personal data' which is treated with heightened protection and includes information such as racial or ethnic origin, religious affiliation, genetic data, health information, and criminal history. Processing of sensitive personal data generally requires explicit consent and carries stricter compliance duties.

Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) excludes purely personal or family use from its regulatory scope. For example, occasional social activity where the data is not shared outside a limited circle.

Core principles of data processing

There are certain core principles to be followed for Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) that govern the lawful collection and processing of personal data. These are as follows:

- Lawfulness, fairness, and transparency: Data must be processed lawfully and fairly with clear communication to individuals about how their data is to be used.
- Purpose limitation: Data must be collected for specific, legitimate purposes and not used in ways incompatible with those purposes. If data is being collected for a newsletter, then it cannot be used for conducting a credit check.
- Data minimisation and accuracy: Organisations should only process data that is adequate and necessary for the purpose and ensure it remains accurate and up to date.
- Storage limitation: Personal data should not be retained longer than necessary.
- Integrity and confidentiality: Adequate security measures must protect data against unauthorised access, alteration, or loss.
- Accountability: Controllers must demonstrate compliance with the law.

These core principles align Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) with global norms seen in regulatory frameworks like the European Union's General Data Protection Regulation (GDPR) positioning Saudi Arabia alongside jurisdictions with advanced data protection standards.

Rights of data subjects

Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) PDPL grants individuals, known as data subjects, certain rights to control how their personal data is processed and these have been illustrated below.

- Right to be informed: Individuals must receive clear information about why their data is being collected, how it will be used, and with whom it will be shared.
- Right of access: Individuals can request access to their personal data and obtain a copy of it in a clear, readable format.
- Right to correction: Inaccurate or incomplete personal data must be rectified upon request.
- Right to deletion: Data subjects can request the destruction of their data when it is no longer required for its original purpose.
- Right to withdraw consent: Consent can be withdrawn at any time for processing that is based on consent.
- Right to restrict processing: Individuals may limit processing when challenging accuracy or legality.
- Right to lodge complaints: Individuals can complain to the relevant authority if they believe their rights under the law have been violated.

Additionally, the law states that data controllers respond to these requests within specified time frames (e.g., 30 days, extendable in certain cases), ensuring operational accountability.

Obligations of data controllers and processors

Under Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443), data controllers, which are defined as entities that determine the purpose and methods of data processing, must ensure compliance with legal bases for processing, such as explicit consent, contractual necessity, or legal obligations. Controllers must maintain comprehensive records of processing activities, detailing data categories, purposes, retention periods, and cross-border transfers. Organisations involved in data collection are generally required to appoint a data protection officer (DPO), implement appropriate security measures and conduct employee training to support compliance. Controllers must also notify authorities of data breaches promptly, particularly when such breaches could harm data subjects. Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) also includes specific requirements for cross-border data transfers which are subject to controls ensuring that data leaving Saudi Arabia continues to receive adequate protection.

Enforcement and penalties

Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) has entered a decisive phase. What began as a framework for future alignment has matured into a live regulatory regime with real enforcement consequences. The Saudi Data and Artificial Intelligence Authority (SDAIA) serves as the initial regulatory body for enforcement, expected to issue further guidelines and oversee compliance. Penalties for non-compliance are significant and include fines up to SAR 5 million (approximately USD 1.33 million) for general breaches of the law, like failing to get consent or implement security etc. It also includes criminal sanctions including fines of up to SAR 3 million (approximately USD 800,000) and imprisonment (up to two years) for unlawful disclosure or publication of sensitive data. Repeating violations may result in double penalties and increased sanctions. Regulators can order mandatory audits, restrict data processing, demand corrective actions, and even suspend operations. By aligning with international best practices, Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) not only protects individuals' privacy rights but also enhances trust, supports international trade, and positions Saudi Arabia as a competitive digital economy ecosystem.

Appointing a data protection officer

The SDAIA issued Rules for Appointing Personal Data Protection Officer in August 2024, effective for mandatory appointment in cases of large-scale processing, systematic monitoring, or sensitive data handling, requiring DPOs with relevant qualifications, integrity, and knowledge of Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443). The requirement to designate a DPO is firmly embedded in the law's framework. Article 30 of Saudi Arabia Cabinet Decision No. 98/1443 (article 30 of Saudi Arabia Royal Decree No. M19/1443) establishes the obligation at the level of primary legislation, while article 32 of Saudi Arabia Administrative Decision No. 1516/1445 Approving the Implementing Regulation of the Personal Data Protection Law elaborates on its application and execution. Under the Saudi regime it identifies specific categories of controllers for whom designation of a DPO is compulsory. These include government and public sector bodies that process personal data extensively, organisations whose activities involve systematic observation or tracking of individuals, entities that handle sensitive personal data as part of their core operations. Once an organisation falls within these categories, the obligation is automatic. There are no threshold-based exemption and no substitute mechanism that allows responsibilities to be informally absorbed by another function without formal designation. This approach reflects a regulatory philosophy that views data protection as a matter of institutional responsibility rather than individual compliance effort. Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) and Saudi Arabia Administrative Decision No. 1516/1445 make it clear that data protection governance is not meant to be abstract or informal. Instead, it must be anchored in a dedicated role with clearly defined authority, expertise, and accountability.

The DPO is the mechanism through which regulators expect organisations to translate legal obligations into daily operational discipline. They position the DPO as an internal advisor who contributes to long-term governance maturity. This includes advising on internal policies and procedures, leading awareness programs and staff training initiatives, reviewing incident response and escalation frameworks, and preparing periodic compliance reports for executive leadership. These duties underscore that the DPO is expected to influence organisational culture, not merely monitor compliance outcomes.

Accountability resting with the data controller and not the DPO alone

A defining feature of Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) is that it does not allow controllers to shift responsibility onto the DPO. While the DPO performs supervisory, advisory, and coordination functions, the legal duty to ensure compliance remains with the data controller. This principle is reinforced through multiple provisions, including articles 4 and 9(6) of the Rules for Appointing Personal Data Protection Officer. These rules emphasise that the controller must ensure that the DPO is capable of performing the role effectively. Appointment alone is insufficient. In practice, this means controllers must take responsibility for selecting a DPO with an appropriate educational and professional background, ensuring the DPO has access to necessary resources, information, and decision-makers, supporting ongoing professional development and skills enhancement, and avoiding conflicts of interest that would undermine the DPO's independence. A nominal appointment designed to satisfy formal requirements, without real authority or support, exposes the organisation to regulatory risk rather than mitigating it.

Qualification and competency expectations

Saudi regulators have been explicit in their expectations regarding the caliber of individuals appointed as DPOs. The Rules for Appointing Personal Data Protection Officer move beyond generic references to "experience" and introduce a more structured standard. The DPO is expected to possess academic grounding relevant to data protection, law, information security, or governance, practical understanding of personal data lifecycle management, familiarity with risk assessment methodologies

and compliance audits along with the ability to interpret legal requirements and translate them into operational controls. Equally important is the expectation of continuous learning. Data protection risks evolve alongside technology, business models, and threat landscapes. The rules therefore require controllers to ensure that DPOs remain current through ongoing training. This reflects a recognition that data protection is not static, and that outdated knowledge can be as damaging as no knowledge at all.

Further, Saudi Arabia Administrative Decision No. 1516/1445 and the Rules for Appointing Personal Data Protection Officer collectively require that the DPO be able to operate without undue influence. This does not mean the DPO must be external or structurally separate, but it does require direct access to senior management, freedom to raise compliance concerns without retaliation, protection from being assigned incompatible operational responsibilities. For example, assigning the DPO concurrent responsibility for revenue generation, marketing strategy, or IT system ownership may compromise objectivity. Regulators are likely to examine such arrangements critically. The Saudi framework therefore treats the DPO as a governance function rather than a technical or administrative role. Article 32(3) of Saudi Arabia Administrative Decision No. 1516/1445 outlines a comprehensive set of responsibilities that collectively define the DPO's mandate. The DPO serves as the primary point of contact with the competent authority. This includes responding to inquiries, coordinating inspections, and facilitating communications related to compliance status, incidents, or corrective actions. This role requires not only legal knowledge but also the ability to represent the organisation accurately and credibly in regulatory engagements. The DPO is tasked with supervising assessments designed to identify and mitigate data protection risks. This includes data protection impact assessments, internal audits, and compliance reviews. The emphasis is on oversight rather than execution. The DPO ensures that assessments are conducted when required, follow appropriate methodologies, and result in meaningful remediation.

Another key responsibility involves enabling individuals to exercise their rights under the Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443). This includes access requests, correction, deletion, and other statutory entitlements. The DPO must ensure that procedures are in place, deadlines are respected, and responses are consistent with legal requirements. Saudi Arabia Administrative Decision No. 1516/1445 assigns the DPO a central role in personal data breach management. This includes coordinating internal response actions, ensuring notifications are made when required, and overseeing corrective measures to prevent recurrence.

The DPO is not expected to handle incidents alone but to orchestrate a structured and legally compliant response across relevant teams. Maintaining accurate records of processing activities is another explicit responsibility. These records are critical during regulatory reviews and demonstrate the organisation's understanding and control of its data ecosystem.

Taken together, Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443), Saudi Arabia Administrative Decision No. 1516/1445 Implementing Regulations, and the Rules for Appointing Personal Data Protection Officer send a consistent message that regulators will assess substance over form. Organisations should expect scrutiny not only of whether a DPO has been appointed, but also of the DPO's qualifications and experience, the level of authority granted to the role, evidence of ongoing training and engagement and the quality of documentation and reporting. Failure in any of these areas may be interpreted as a failure of governance, even if no specific data breach has occurred. Therefore, for organisations operating in the Kingdom or processing data related to Saudi residents, the DPO should be viewed as a strategic investment rather than a regulatory cost.

Conclusion

Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) represents a foundational shift in how personal data is governed, protected, and trusted within the Saudi digital ecosystem. As part of the broader Vision 2030 agenda, the Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) signals the Kingdom's commitment to building a secure, transparent, and globally credible data economy that balances innovation with individual privacy rights. By introducing a comprehensive statutory framework with extraterritorial reach, clearly defined processing principles, enforceable data subject rights, and robust obligations on controllers and processors, the law elevates data protection from a policy aspiration to a binding legal duty. The alignment of Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) with internationally recognised standards, particularly those reflected in regimes such as the GDPR[1 p.6], facilitates cross-border commerce, supports foreign investment, and enables Saudi-based organisations to integrate more seamlessly into global data-driven markets. With enforcement now active and penalties carrying both financial and criminal consequences, compliance with Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) is no longer optional or theoretical. Organisations operating in or targeting the Saudi market must embed data protection into their governance, operational processes, and corporate culture. Further, Saudi Arabia Cabinet Decision No. 98/1443 (Saudi Arabia Royal Decree No. M19/1443) marks a clear evolution in regional data protection regulation as appointment of the DPO is no longer an optional safeguard or a symbolic title. It is a central pillar of the Kingdom's data governance architecture. By requiring qualified individuals, continuous capability building, and genuine organisational support, the Saudi framework makes clear that effective data protection must be embedded at the heart of corporate governance.

Author

Rajiv Suri
Senior Associate, Alsuwaidi & Company LLC (UAE)
r.suri@alsuwaidi.ae
+971545831894

Areas of expertise

Intellectual Property; Corporate.

Education

B.Sc (Hons), LL.B, Delhi University.

Memberships

- Bar Council of Delhi, India.
- Authorised Legal Consultant by Legal Affairs Department, Government of Dubai, UAE.

Biography

Rajiv is one of the leading expert lawyers with over 29 years of experience specialising in the field of Intellectual Property laws, Commercial and Transactional laws including contracts, information technology and media. He holds degree in Sciences and Law. He qualified as a lawyer in 1994 and since then has practiced as an Advocate/Legal Consultant.

His expertise lies at handling both contentious and non-contentious issues both in India and UAE. Rajiv advice clients on strategies involving a wide range of intellectual property matters and has been involved in managing corporate portfolios across various industries.

He has also dealt extensively on commercial and transactional matters involving drafting and vetting varied forms of commercial agreements/contracts, technical knowhow agreements, licensing issues including third party/vendor contracts, non-disclosure agreements, manufacturing of goods agreement, business development and service agreement, brand acquisition agreement, assignment deed/s, drafting and execution of Wills in UAE etc.

He has been an author/co-author of articles relating to intellectual property issues and corporate matters for some of the leading legal publications. He has been a speaker at webinars/round table/s on issues relating to intellectual property rights and non- muslim personal law in UAE.

His name appears in UK's whoswholegal.com (WWL) 2008 for UAE, as a ranked prosecution lawyer in Managing Intellectual Property (MIP) 2019, in the list of World's Leading Trademarks professionals by World Trademarks Review (WTR) for the years 2020, 2021, 2022 & 2023 (UAE) and in the list of IP experts compiled by AsiaIP for the years 2021 and 2022.

Rajiv is fluent in English and Hindi.

Notes

1. ^ [p.4] https://gdpr-info.eu/