IN-DEPTH

Artificial Intelligence Law

SAUDI ARABIA

LEXOLOGY

Artificial Intelligence Law

EDITION 3

Contributing Editors
Karen Silverman and **Emily Caplan**
The Cantellus Group

In Depth: Artificial Intelligence Law is a perceptive global overview of the fast-evolving state of law and practice surrounding artificial intelligence (AI) systems and applications. Focusing on recent developments and their practical implications, it examines key issues including legislative initiatives, government policy, AI risk management principles and standards, enforcement actions and much more.

Generated: November 24, 2025

Saudi Arabia

Brian Meenagh, **Harj Rai**, **Marc Makary**, **Ksenia Koroleva** and **Faisal Imam**
Latham & Watkins LLP

Summary

Introduction

Artificial intelligence (AI) remains a core pillar of Saudi Arabia's Vision 2030;[1] 66 of the 96 strategic objectives set out in the plan are in respect of AI and data. Saudi Arabia continues to combine large-scale investment and public–private partnerships with an increasingly detailed regulatory framework designed to position Saudi Arabia as a global leader in responsible AI adoption.

The Saudi Data and Artificial Intelligence Authority (SDAIA) leads this agenda, including through the development of the National Strategy for Data & AI, of which one of the objectives is to "stimulate data and AI adoption through the creation of a collaborative and forward-thinking ecosystem that will drive commercialization and industry application of data and AI". The SDAIA also has a dedicated National Center for Artificial Intelligence, which is tasked with AI research and solutions development, providing AI strategic advice to the government, and promoting AI education and awareness.

The AI regulatory landscape has evolved in 2024 and 2025. SDAIA finalised the AI Ethics Principles (September 2023) and followed with practical guidance for generative AI with the publication of the Generative AI Guidelines (January 2024). The Personal Data Protection Law (PDPL) entered into force with enforcement commencing after the one-year transition period (mid-September 2024). A draft Global AI Hub Law (April 2025) proposes a first-of-its-kind, comprehensive framework for 'data embassies' and AI hub categories in Saudi Arabia. Sectoral rules on media content, cybersecurity and competition continue to interact with AI deployments, and intellectual property policy is evolving to address AI-generated works.

Year in review

Technology

The AI industry is developing on a global basis, with regional and local divergence driven predominantly by policy and regulatory factors, rather than technical factors. The headline trend of the last year – both globally and in Saudi Arabia – has been the advancement of international projects, particularly in the realm of digital infrastructure related to artificial intelligence. This includes significant investments in data centres, which serve as the backbone for AI operations by providing the necessary computational power and storage capabilities. This has driven greenfield builds and upgrades to increase GPU capacity, adopt advanced cooling and energy-efficiency designs, and deploy low-latency interconnects, often pursued through public–private partnerships. Additionally, there has been a concerted effort to develop large language models (LLMs), with Saudi Arabia taking notable strides in creating its own Arabic language LLMs. These initiatives not only aim to enhance the region's technological capabilities but also to position Saudi Arabia as a leader in AI innovation within the Arabic-speaking world. By focusing on these international projects, Saudi Arabia is contributing to the global AI landscape while addressing regional needs and linguistic diversity.

Key policy and legislative developments:

- Generative AI Guidelines (January 2024). SDAIA issued two Generative AI Guides, one for government employees and one for the public. They define generative AI, set out risk themes (e.g., data leakage, misinformation, deepfakes), recommend mitigations, and require government bodies to implement responsible use policies, training and compliance programmes that align with the AI Ethics Principles. The public-facing guide recommends, among other measures, content moderation, know-your-customer (KYC) protocols for cloud service providers, and human-in-the-loop controls.
- AI Adoption Framework (September 2024). SDAIA's framework complements the AI Ethics Principles, primarily by mapping lifecycle practices and governance; it does not introduce additional binding obligations but is helpful for implementation.
- Draft Global AI Hub Law (April 2025). The Communications, Space and Technology Commission (CST) published a consultation draft of a Global AI Hub Law, proposing a 'data embassy/ ecosystem and a comprehensive framework to categorise and establish sovereign AI/data hubs in Saudi Arabia. The consultation closed on 14 May 2025.

Legislative and regulatory framework

Ethics principles

The AI Ethics Principles apply broadly to any stakeholders designing, developing, deploying, implementing, using, or affected by AI systems in Saudi Arabia, across public and private sectors. SDAIA is tasked with 'monitoring compliance', including audits and coordination with sectoral regulators. While the Principles themselves do not create standalone penalties, non-compliance can heighten risk under adjacent legal frameworks (e.g., PDPL).

The AI Ethics Principles adopt a lifecycle model – plan and design; prepare input data; build and validate; deploy and monitor – and introduce risk categories: little/no risk, limited risk, high risk (subject to pre- and post-conformity assessments) and unacceptable risk (e.g., social profiling, exploitation of children, behaviour distortion).

Adopting entities should designate the following roles:

- Head of entity/chief data officer: primary SDAIA contact, accountable for AI ethics practices and approves annual AI ethics reporting.
- Chief compliance officer/compliance officer: strategic AI ethics champion ensures alignment with national regulations, including privacy and data classification; oversees third-party adherence.
- Responsible AI officer: operational lead and drives AI ethics plans, procedures, KPIs and staff training in coordination with data management.
- AI system assessor: independent auditing of AI systems, periodic reviews and KPI monitoring and audit reporting.

The AI Ethics Principles include optional registration with SDAIA, an AI ethics checklist (can be conducted via the National Governance Platform) mapped to lifecycle phases and detailed tools for fairness, algorithm assessment and privacy/security by design measures, with references to recognised standards.

Under the AI Ethics Principles, entities should manage AI risks and impacts across the lifecycle by implementing controls for:

- Fairness, bias, and discrimination
- Eliminate bias and discrimination across the lifecycle, conduct fairness assessments and avoid sensitive attributes where appropriate.
- Humanity. Ensure systems are ethically permissible and aligned with human rights and cultural values, with governance to assess societal impact.
- Social and environmental benefits. Contribute to social and environmental progress and avoid accelerating harm; conduct continuous impact assessments.
- Reliability and safety. Design for robustness, manage outliers and include human oversight for high impact decisions; prohibited uses include social scoring and mass surveillance.
- Transparency and explainability. Inform stakeholders about purposes, data and decision rationale; maintain logs; establish issues/complaints processes; and adhere to IP and data privacy standards.
- Accountability and responsibility. Define roles, responsibility and liability at design; embed data quality checks and bias remediation; and pre-define alerts for performance drift.

Generative AI Guidelines (January 2024)

SDAIA issued two complementary Generative AI Guides in January 2024 – one tailored to government entities and one for the general public. Together, these guides advance responsible adoption of generative AI in Saudi Arabia, align practices with the AI Ethics Principles and address distinct audiences and use contexts.

The Government Guide binds government entities and indirectly any parties processing, issuing or storing government data. It mandates adherence to the AI Ethics Principles, adoption of internal policies for responsible generative AI use, legal compliance (privacy, data classification) and periodic employee training.

The Public Guide applies to all stakeholders in generative AI development and use. It emphasises risk identification (e.g., hallucinations, misinformation, deepfakes), recommends mitigations (e.g., accuracy estimation, source citation where possible, pre-defined warnings when accuracy is low, watermarking) and promotes user education and content moderation. For cloud providers, it encourages KYC and prohibited content filtering.

AI Adoption Framework (September 2024)

The AI Adoption Framework operationalises the AI Ethics Principles and cross-refers to them extensively. It is helpful for governance design and internal adoption programmes, though it does not impose new obligations.

Draft Global AI Hub Law (April 2025): data embassies and AI hubs

Saudi Arabia's draft Global AI Hub Law pioneers a comprehensive 'data embassy' and AI hub regime, aiming to:

- reinforce Saudi Arabia's position as a global AI and advanced technology hub;
- leverage Saudi Arabia's geographic position and infrastructure for global digital services; and
- facilitate sovereign data centres and structured international cooperation.

The draft law defines three AI Hub categories, each of which may comprise a full data centre or an isolated, clearly demarcated segment:

- Private hub. Operated by a 'guest country' for its exclusive use under that country's laws and regulations, pursuant to a bilateral agreement with Saudi Arabia.
- Extended hub. Operated by a third-party 'operator under agreement with a Saudi 'competent authority' and arrangements with a guest country, subject to the guest country's laws.
- Virtual hub. Operated by a Saudi-based 'service provider' approved by the competent authority to offer a virtual hub to 'customers', governed by the laws of a 'designated foreign state'. Customer content would fall under the jurisdiction of the competent courts of the designated foreign state, while Saudi courts can provide necessary assistance.

Guest countries are responsible for ensuring compliance with international law, adhering to technology-use restrictions, and cooperating with Saudi authorities. The competent authority (to be designated by the Council of Ministers) may engage in negotiations and enter agreements to establish hubs. Future implementing regulations are expected to clarify setup processes, distinctions among hub categories, and operational controls. As a first step towards a data embassy ecosystem, this draft is notable and groundbreaking among G20 jurisdictions.

Managing AI risks and impacts

Data protection

AI Ethics Principles

As per the AI Ethics Principles, AI systems must be built in a way that respects the privacy of data collected and upholds data security. Relevant controls include:

1. planning and designing the AI system so that there is respect for the privacy of individuals; and

2. ensuring that:

- automated decision-making is not based on personally identifying characteristics;
- data minimisation and de-identification are applied to personal data;
- data classification is applied;
- privacy and security by design is implemented; and
- a privacy impact assessment and risk management assessment are carried out.

There is a prohibition against designing AI systems that result in profiling individuals or communities, unless approved by the chief compliance and ethics officer or compliance officer, or in compliance with a code of ethics issued by a sector regulator. There is also a prohibition on using AI systems for social scoring or mass surveillance purposes.[2]

The PDPL is Saudi Arabia's comprehensive data protection regime, consisting of the primary law and its Implementing Regulations (including the Regulations on Personal Data Transfers outside Saudi Arabia). It applies to any processing of personal data in Saudi Arabia, and extraterritorially to processing of data about individuals residing in Saudi Arabia. Core principles include transparency, purpose limitation, data minimisation and security. Lawful bases include consent, contractual necessity and legitimate interests, among others. Controllers must provide privacy notices and enable data subject rights (information, access, correction).

Where decisions are made solely through automated processing, the PDPL and its Implementing Regulations require particular care, including – depending on context – 'explicit consent' where consent is the chosen lawful basis. SDAIA's Generative AI Guidelines further recommend that service providers give users meaningful choices, including the option to refuse the use of their data for model training.

Personal Data Protection Law

The PDPL is Saudi Arabia's comprehensive data protection regime, consisting of the primary law and its Implementing Regulations (including the Regulations on Personal Data Transfers outside Saudi Arabia). It applies to any processing of personal data in Saudi Arabia, and extraterritorially to processing of data about individuals residing in Saudi Arabia.

A number of PDPL requirements will affect AI systems directly if these involve the processing of personal data. Examples of key legal requirements to note include:

1. data processing principles: the PDPL includes a number of principles, such as transparency, purpose limitation, data minimisation and security, which are similar to requirements set out in the AI Ethics Principles;[3]
2. legal basis: data controllers require a legal basis for processing personal data, which includes consent of the individual, contractual necessity and legitimate interests. A legal basis will need to be in place for all processing of personal data in relation to AI systems.[4] Noting that where decisions are made solely through automated processing, the PDPL require particular care, including – depending on context –'explicit consent' where consent is the chosen lawful basis. SDAIA's

Generative AI Guidelines further recommend that service providers give users meaningful choices, including the option to refuse the use of their data for model training.

3. data subject rights: individuals have rights in relation to their personal data, including the right to be informed about the processing via a privacy notice, the right to access their personal data and the right to correct their personal data. These rights must be taken into account for AI systems, and link to Principle 6 in the AI Ethics Principles, on transparency and explainability;[5]
4. sensitive data: a number of categories of personal data are defined as sensitive and are subject to more stringent requirements under the PDPL and specific requirements under the AI Ethics Principles. Examples of sensitive data include a person's ethnic origin, religious or political beliefs, health data, criminal offences data and biometric data. Note that location data and credit data are also considered sensitive under the AI Ethics Principles, but are not sensitive under the PDPL (although additional controls apply to credit data);[6]
5. data protection impact assessment: controllers must conduct an impact assessment regarding personal data processing in relation to high-risk products and services, which includes any processing of sensitive data, collecting or comparing two or more data sets, processing using new technologies, or making decisions based on automated processing of personal data.[7] This requirement is highly likely to be relevant to AI systems, in particular given the use of new technologies involved, and the use of AI for automated decision-making; and
6. international transfers: controllers must satisfy purpose requirements for a transfer outside of Saudi Arabia. SDAIA has not yet published the adequacy list and until then, controllers generally rely on alternatives, including standard contractual clauses, binding common rules for such transfers, or (in future) importer certification. Transfer risk assessments (TRAs) are required in specified scenarios, including when relying on SCCs/BCRs/certification, and when transferring sensitive data on a continuous or widespread basis.

Intellectual property

Saudi Arabia is a party to many international treaties regarding the protection of intellectual property rights and has a number of laws and regulations implementing advanced rules for different types of intellectual property, including patents, trademarks, copyright and trade secrets.[8]

The intellectual property regime in Saudi Arabia does not have separate rules regarding AI; nevertheless:

1. it recognises only persons (rather than machines or algorithms) participating in the creation of works as authors; and
2. it implements a number of concepts relevant to intellectual property rights in the context of AI; for example, the Copyright Law[9] has a concept of 'lawful use' relevant to the use of background content. This concept allows fair use of copyrighted material for personal use, educational purposes or limited quotation.

In the context of training large language models, copyright considerations are particularly salient. Unlike some jurisdictions (such as the United States), the Saudi Arabian Copyright Law does not recognise a generalised 'transformative use' limb as part of lawful use analysis. As a result, developers cannot assume that ingesting copyrighted web content for training will be defensible on a transformative-use theory. Instead, risk analysis should focus on whether training inputs fall within one of the enumerated lawful use categories or are licensed, and whether technical and organisational measures minimise the likelihood of memorisation and regurgitation of protected expression.

The key authority in respect of intellectual property protection is the SAIP. Its aims are to "regulate, support, develop, sponsor, protect, enforce and upgrade the fields of intellectual property in the Kingdom in accordance with international best practices".[10] Saudi Arabia has published a National Intellectual Property Strategy (NIPST),[11] which aims to support innovation and creativity and make Saudi Arabia a leader in intellectual property.

In April 2023, the SAIP published a draft set of amendments to intellectual property legislation for public consultation (which remained open until May 2023). The aim of the draft was to harmonise the various existing intellectual property laws and regulations and, *inter alia*, contained a section on intellectual property rules on AI titled 'AI-related IP and emerging technologies, and support their motivation'. Pursuant to the draft regime, AI cannot be treated as author – only an individual can be an author of content protected by intellectual property rights, in particular:

1. intellectual property protection is granted to content to which the contribution of an individual is 'prominent', in which case intellectual property rights pertain to the relevant person or another person making arrangements towards ownership of intellectual property (e.g., an employer);
2. content is not protected by intellectual property rights, and enters the public domain, if the contribution by individuals is not prominent or if the content was created by AI independently of an individual; and
3. the notion of 'prominence' is not determined in the draft regime; however, it is likely to be a matter for assessment case by case.

The AI Ethics Principles also refer to intellectual property in connection with transparency and explainability, with a requirement for input data to be acquired and collected in adherence with intellectual property standards and controls.[12]

Liability

The AI Ethics Principles set normative standards without their own penalties, and the Generative AI Guidelines similarly do not enumerate specific penalties or an independent enforcement regime. In practice, compliance expectations under both instruments are likely to be driven through audits, policy adoption requirements (particularly for government entities), and the application of existing statutes. That being said, the laws of Saudi Arabia include rules on liability that may be triggered by the development and use of AI and AI systems; for example, the PDPL contains a number of significant and onerous penalties for non-compliance, which could be triggered where personal data is processed for AI purposes. Key enforcement powers under the PDPL to note include:

1. Article 35(1): disclosure of sensitive data in breach of the PDPL with the intention to cause harm to the relevant data subject or to gain a personal benefit may result in up to two years' imprisonment or a fine of up to 3 million riyal, or both;
2. Article 36: all other matters of non-compliance may result in a warning or a fine of up to 5 million riyals, which may be doubled for repeat offences;
3. Article 38: a competent court may order the confiscation of funds obtained as a result of a violation; and
4. Article 40: individuals can make compensation claims for material or moral damage.

The Copyright Law[13] provides for liability in the form of a warning, a fine of up to 250,000 riyals, closure of the infringing entity for up to two months, confiscation of infringing material, or imprisonment for up to six months for a first-time offence, which may be doubled for a repeat offence. These penalties may apply if background content infringes third-party intellectual property rights or exceeds the scope of permitted use.

The Anti-Cyber Crime Law[14] imposes penalties of up to 3 million riyals for a number of actions defined as cybercrimes, including inflicting damage on others through the use of information technology devices. These penalties may apply if AI systems are used to commit the relevant offence.

A draft Consumer Protection Law, published by the Ministry of Commerce in March 2022,-[15] provides for possible penalties in the form of a warning, a fine of up to 100,000 riyals, suspension of business activities and temporary or permanent prevention of the provision of the system used in the infringement. These penalties may apply, for example, in the event of a failure to disclose information to consumers regarding the use of AI.

Fraud and consumer protection

Saudi Arabia is working on its consumer protection laws. According to the draft Consumer Protection Law, a number of activities directed at consumers (persons acquiring goods or services for personal needs) are prohibited, in particular unfair or misleading commercial practices, which include incidences of false information being given or information being provided in any way that deceives consumers, omits relevant information or gives information in an unclear or unintelligible manner. Consumers also have the right to information required to enable them to make an informed choice according to their wishes and needs and the right to be informed of the consequences of the choices they make.

Echoing these requirements with respect to AI, under the AI Ethics Principles, individuals are included in the terms 'adopting entity' and 'end user'. Entities developing the use of AI need to adhere to certain principles with regard to interacting with end users and ensure that end users are provided with full information about the AI system in question.

The Generative AI Guidelines are also relevant. They recommend that publicly available generative AI services estimate the accuracy of information before display, cite sources where possible, warn users with pre-defined messages when accuracy is low, embed watermarks in outputs, and provide regular reminders to verify content. They also encourage clear disclosures about AI use to help users make informed choices and,

for cloud providers, KYC and prohibited-content filtering. While these expectations are not paired with standalone penalties, failure to implement them can increase risk under existing laws when AI outputs mislead users or disseminate unlawful content.

Disclosure and notice-of-use requirements

See under 'Fraud and consumer protection' above.

Jurisdiction

The jurisdictional scope of technology rules in Saudi Arabia is generally broad. The AI Ethics Principles apply to any persons designing, developing, deploying, implementing, using, or being affected by AI systems within Saudi Arabia, across public and private sectors. The PDPL likewise applies to any processing of personal data carried out in Saudi Arabia, and extraterritorially to processing of personal data relating to individuals residing in Saudi Arabia by entities outside the Kingdom.

SDAIA's Generative AI Guidelines add a further layer: the Government Generative AI Guide is mandatory for government entities and indirectly captures vendors and other parties that issue, process, or store government data; the Public Generative AI Guide sets baseline expectations for all stakeholders involved in generative AI development and use. While the Public Guide does not establish standalone penalties, both guides are expected to be applied and overseen via existing legal frameworks and administrative supervision (e.g., audits and policy requirements).

Other

Cybersecurity

Saudi Arabia's National Cybersecurity Authority (NCA) updated its core frameworks in 2024, including the Essential Cybersecurity Controls (ECCs) and the Cloud Cybersecurity Controls (CCCs). The ECCs are mandatory for government entities (including government-owned companies) and for private-sector operators that own, operate, or host critical national infrastructure; they are recommended for other organisations as baseline controls. The CCCs set requirements specifically for cloud service providers and cloud customers in scope of the NCA regime, with emphasis on governance, data protection, tenant isolation, and monitoring in cloud environments. Notably, according to the 2024 updates, competencies relating to data localisation and data management have been moved to the National Data Management Office (NDMO) at SDAIA, and entities should assess localisation and data-sovereignty issues under NDMO frameworks and any applicable sectoral rules. The NCA's Critical Systems Cybersecurity Controls (CSCCs) continue to apply to any organisation that owns or operates 'critical systems', i.e., systems whose failure, unauthorised change, or unauthorised access could materially disrupt services or cause broader economic, security or social harm. AI systems that underpin critical operations may fall in scope of the CSCCs, triggering additional controls, including strict remote access constraints and heightened security governance.

Regulatory sandboxes and dialogue

There has been an increase in the availability and use of sandboxes in Saudi Arabia to balance innovation with oversight, including:

- SDAIA's Data and Privacy Regulatory Sandbox. Supports testing of data driven solutions in a supervised environment with PDPL compliance guardrails. Current cohorts have focused eligibility on micro, small and medium-sized enterprises as defined by Monsha'at. Monsha'at, officially known as the Small and Medium Enterprises General Authority, is a government agency in Saudi Arabia dedicated to supporting and promoting the growth of small and medium-sized enterprises within the country.
- CST's Emerging Technology Regulatory Sandbox. Caters to startups, SMEs, and established firms to test AI, IoT, and cloud solutions, with cohort-based admissions.

Even where participation is not feasible, early regulatory engagement, optional SDAIA registration (under the AI Ethics Framework), and the use of SDAIA's AI Ethics Assessment Tool (via the National Data Governance Platform) can help align deployments with expectations.

Enforcement

There is limited AI-specific enforcement in Saudi Arabia at the time of writing.

For example, a 9,000 riyals fine was imposed on an individual for violating copyright law by modifying a personal photograph using artificial intelligence (AI) and republishing it without the original owner's consent. This case, announced by the SAIP, is one of the first publicly reported penalties in Saudi Arabia involving AI misuse in a copyright context.

The violation occurred when the individual altered a personal image with AI tools and exploited it commercially, which SAIP identified as a clear breach of Saudi Arabia's Copyright Law. The process began with a complaint from the copyright holder, followed by an investigation and questioning of the accused, who was allowed to present a defence. A specialised committee confirmed the violation and issued the financial penalty.

SAIP emphasised that using AI to manipulate or repurpose personal content without authorisation does not exempt individuals or institutions from legal responsibility.

This development, although not directly related to more pertinent issues like AI model training, indicates a growing regulatory focus on AI technologies, and highlights that AI is on the minds of regulators.

Legal practice implications

Since the surge in generative AI, there has been an influx of new AI and generative AI-based legal technology in Saudi Arabia, adding to the first wave of earlier AI legal technology. General AI applications – not specific to the legal market – are also used widely in a legal context, though demand for legal practice-specific AI tools is high, given the particular

demands, such as high standards for accuracy, explainability and information security, and the specific nature of legal practice use cases.

Along with other professional services, the legal vertical has been among the first to experience significant growth in AI tools, in this latest wave of powerful AI systems, in part due to the large number of activities across legal practice that can be accomplished more efficiently or effectively by AI, and the fact that those activities are typically relatively high value. These characteristics result in a market that is ripe for industry-specific AI innovation. AI legal technology is growing across nearly all areas of the legal market, from contentious practices to advisory and commercial matters. Similarly, AI tools are proliferating on both the client-facing side (from contract drafting and due diligence, to legal research, discovery and court ruling predictions) and on the legal practice management and operations side (in areas such as fees and financing, knowledge management and document management).

There are certain barriers to change within the AI legal technology market, in Saudi Arabia and elsewhere, including challenges in achieving frictionless end-to-end AI legal processes. AI legal tools typically address inefficiencies in a particular task or stage of a legal process (for example, reviewing a document, documenting changes to a document or simultaneously amending a large number of documents) but do not address the process end-to-end or with interoperability. This leaves certain residual inefficiencies and bandwidth issues in the process as a whole. In addition, multi-sided and multi-party AI legal technology requires a critical mass of engagement for the technology to supersede the previous, off-tech process. It may take a while for the latest wave of AI legal technology to achieve that critical mass in Saudi Arabia and global legal markets, but AI tools look set to be ultimately transformative across legal practice.

Outlook and conclusions

Two trajectories remain clear:

1. Saudi Arabia – across public and private sectors – will continue to invest heavily in AI technology and infrastructure through investment and partnerships with foreign technology companies and local joint ventures seeking to harness the benefits of AI for local use in Saudi Arabia; and
2. SDAIA, SAIP and other regulators will issue additional laws and regulations focusing on the development, operation and use of AI technology in Saudi Arabia.

It would not be surprising to see a specific law issued with respect to the use of generative AI for digital content and liability where the content is not compliant with criminal laws or content standards in Saudi Arabia. The draft Global AI Hub Law signals Saudi Arabia's ambition to pioneer legal infrastructure for sovereign data and cross-border digital operations, positioning Saudi Arabia at the centre of global AI ecosystem.

Endnotes

1 See https://www.vision2030.gov.sa/en/vision-2030/overview. ^ Back to section

2 id., p. 22. ^ Back to section

3 PDPL, Articles 11, 14, 18 and 19. ^ Back to section

4 id., Articles 5 and 6. ^ Back to section

5 id., Articles 4 and 12, and PDPL Implementing Regulations, Articles 3–8. ^ Back to section

6 PDPL, Article 1(11) and AI Ethics Principles, p. 7. ^ Back to section

7 PDPL, Article 22. ^ Back to section

8 https://www.saip.gov.sa/en/privacy-legislation/#regulations_and_regulations. ^ Back to section

9 Copyright Law, issued by Royal Decree No. M/ 41 dated 2/7/1424 AH (corresponds to 30 August 2003), as amended by Cabinet Resolution No. 536 dated 10/19/1439 AH (corresponds to 3 July 2018), available at https://externalportal-backend-production.saip.gov.sa/sites/default/files/2023-02/%D8%AD%D9%82%D9%88%D9%82%20%D8%A7%D9%84%D9%85%D9%88%D9%94%D9%84%D9%81_0.pdf. ^ Back to section

10 https://www.my.gov.sa/wps/portal/snp/agencies/agencyDetails/AC415. ^ Back to section

11 See https://www.spa.gov.sa/w1829966 and https://www.saip.gov.sa/en/national-strategy/. ^ Back to section

12 AI Ethics Principles, p. 24. ^ Back to section

13 See supra n. 23. ^ Back to section

14 Issued under the Council of Ministers Decision No. 79, dated 7/3/1428 H (corresponds to 26 March 2007), and approved by Royal Decree No. M/17, dated 8/3/1428 H (corresponds to 27 March 2007), available at https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/2. ^ Back to section

15 https://istitlaa.ncc.gov.sa/en/Trade/mci/Consumer/Pages/default.aspx. ^ Back to section

LATHAM & WATKINS LLP

Brian Meenagh	brian.meenagh@lw.com
Harj Rai	harjaskaran.rai@lw.com
Marc Makary	marc.makary@lw.com
Ksenia Koroleva	ksenia.koroleva@lw.com
Faisal Imam	Faisal.Imam@lw.com

Latham & Watkins LLP