IN-DEPTH

Artificial Intelligence Law

SAUDI ARABIA

LEXOLOGY

Artificial Intelligence Law

EDITION 1

Contributing Editors

Karen Silverman and **Brinson Elliott**

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: January 17, 2024

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information.

LEXOLOGY

Saudi Arabia

Brian Meenagh, Ksenia Koroleva and Lucy Tucker
Latham & Watkins LLP

Summary

Introduction

Artificial intelligence (AI) is a core pillar of Saudi Arabia's Vision 2030:[2] 66 of the 96 strategic objectives set out in the plan are in respect of AI and data. The strategy involves overseas investment, development of local AI companies and the creation of a regulatory environment that will position Saudi Arabia as a forward-thinking jurisdiction for the adoption of AI.

Saudi Arabia has created a specific authority, the Saudi Data and Artificial Intelligence Authority (SDAIA), to 'drive the national agenda for Data & AI to elevate the Kingdom as a global leader in the elite league of data driven economies'.[3]

The SDAIA has developed 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.

There were two specific major developments in AI-related jurisprudence in Saudi Arabia in 2023. First, in April 2023, the Saudi Authority for Intellectual Property (SAIP) published a draft set of amendments to intellectual property legislation for public consultation. The aim of the draft was to harmonise the various existing intellectual property laws and regulations. Among other things, it contained a section on intellectual property rules on AI titled 'AI-related IP and emerging technologies, and supporting their motivation'.

In September 2023, the SDAIA issued the final version of its AI Ethics Principles (Version 1.0).[4] These represent the first AI legal framework in Saudi Arabia and define AI ethics as 'a set of values, principles and techniques to guide moral conduct in developing and using AI technologies'.[5]

This chapter provides further information about both these developments and addresses other key regulatory developments, including data privacy, applicable to AI law in Saudi Arabia.

Year in review

i 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 - is the proliferation of accessible generative AI systems. This new world of generative AI has given rise to intense and divisive debate at policy, regulatory, and social levels in an array of areas from individual privacy and the protection of human creativity, to existential questions of truth and reality. More recently, enterprise integration has emerged as a key technological shift, as the main providers in the enterprise SaaS and PaaS markets integrate generative AI systems into their core products. Prevalent uses cases for natural language processing and generation

AI tools include chatbots and conversational AI (e.g., used in customer service), automated speech/ voice recognition, and translation tools.

ii Developments in policy and legislation

As stated in Section I, the SDAIA issued the final version of its AI Ethics Principles in September 2023. The Principles had previously been issued for consultation and the final version represents the first AI legal framework in Saudi Arabia.

In March 2023, an amended version of the Personal Data Protection Law[6] (PDPL) was issued (pursuant to Royal Decree No. M/148 of 05/09/1444 H) and, in September 2023, following a public consultation, the Implementing Regulation was also issued.[7] The PDPL came into force on 14 September 2023 but there is a one-year transition period for compliance, which ends in mid September 2024. The PDPL applies to any processing of personal data by any means that takes place in Saudi Arabia, including any processing of personal data relating to individuals residing in Saudi Arabia by entities outside Saudi Arabia.[8] Although not specific to AI, a number of PDPL requirements will affect AI systems where these involve the processing of personal data.

Legislative and regulatory framework

The new AI Ethics Principles are the key regulatory framework for AI. They are not legally binding and we are not aware of the SDAIA having enforcement powers specifically in relation to the Principles; however, non-compliance could trigger enforcement and penalties in relation to other legal requirements, such as the PDPL.

We are not aware of any other AI-specific laws in Saudi Arabia.

The new AI Ethics Principles are the key regulatory framework for AI. They are not legally binding and we are not aware of the SDAIA having enforcement powers specifically in relation to the Principles; however, non-compliance could trigger enforcement and penalties in relation to other legal requirements, such as the PDPL.

We are not aware of any other AI-specific laws in Saudi Arabia.

i Scope

The Principles have a very broad scope and apply to AI stakeholders who are designing, developing, deploying, implementing, using or being affected by AI systems within Saudi Arabia, including individuals and legal entities, in both the public and private sectors.[9]

ii Enforcement bodies

In the Principles, the SDAIA is described as working to 'monitor compliance' with the Principles. The SDAIA's powers include measuring compliance of in-scope entities and individuals based on the 'defined compliance mechanism' (although this is not set out in detail) or through sector regulators, and auditing AI ethics activities when required. The SDAIA may conduct investigations and audits and monitor compliance with the Principles with the support of other relevant national regulators.[10]

The SDAIA may issue motivational badges to prompt entities and reflect the level of their compliance and progress with the adoption of AI ethics.[11]

iii Risk categorisation

The Principles classify the risks associated with the development and use of AI, using the following categories:

1. Little or no risk: There are no restrictions on such systems but it is recommended that they are ethically compliant. An example is a spam filter.
2. Limited risk: These systems are subject to the Principles. An example is technical programs relating to function, development and performance.
3. High risk: These systems must undergo pre- and post-conformity assessments, in addition to adhering to ethics and the relevant statutory requirements. No examples are provided but these systems are described as posing a high risk to basic rights. No further details are provided on conformity assessments, although the Principles do refer to other assessments, such as AI ethics assessments, privacy impact assessments and risk management assessments.
4. Unacceptable risk: These systems are not allowed because they pose an unacceptable risk to people's safety, livelihood or rights, such as systems relating to social profiling, the exploitation of children or the distortion of behaviour.[12]

iv Other requirements

Internal roles

Adopting entities (i.e., within the scope of the Principles) must designate individuals who are responsible for carrying out AI ethics activities within the following roles:

1. head of the entity or chief data officer, to be responsible for AI ethics practices within the entity and the first point of contact with the SDAIA;
2. chief compliance officer or compliance officer, to be the strategic lead for AI ethics and whose responsibilities include ensuring the compliance of AI activities with other national regulations, including on data privacy;
3. responsible AI officer, to be the operational lead of responsible AI; and
4. the AI system assessor, to be responsible for auditing AI systems.[13]

Optional registration

The Principles include an optional registration and the stated aim is to motivate entities to consider AI ethics. The SDAIA may follow up and measure the commitment and compliance of registered entities and provide support, including making recommendations regarding compliance with AI ethics.[14]

v AI ethics tools and checklist

The Principles include an Annexure, which describes various tools relating to AI ethics, including a public-facing AI Fairness Position Statement; an Ethical Impact Assessment; compliance with privacy and security standards, such as ISO standards on AI and the US National Institute of Standards and Technology's Cybersecurity Framework; an Algorithm Assessment; a Fairness Assessment to compare how fair models perform for specific groups (with references to online tools available for this purpose); and examples of data protection methods, including anonymisation and encryption.[15]

There is a further Annexure that sets out the above AI ethics tools and how they map with the AI system life cycle, to show at which phase they are relevant.[16]

The Principles also include an AI Ethics Checklist for each of the four life cycle phases, which links relevant questions (e.g., Did you design the appropriate level of human oversight for the AI system and use case?) to the relevant principles and states whether they are binding for third parties.

Managing AI risks and impacts

The AI Ethics Principles set out controls that should be implemented, in relation to each principle, for each step of the AI system life cycle, which is comprised of four steps: plan and design; prepare input data; build and validate; and deploy and monitor.

The AI Ethics Principles set out controls that should be implemented, in relation to each principle, for each step of the AI system life cycle, which is comprised of four steps: plan and design; prepare input data; build and validate; and deploy and monitor.

i Fairness, bias and discrimination

Principle 1 relates to fairness,[17] which requires in-scope entities to take the necessary actions to eliminate bias, discrimination or stigmatisation of individuals or groups at each step of the AI system life cycle. Relevant controls include conducting a fairness assessment of the AI system, following best practice in terms of responsible data acquisition and data quality, excluding sensitive personal data attributes relating to disadvantaged individuals or groups, and assessing the outcomes of the predictive model in respect of represented groups.

Principle 3, on humanity, is also relevant.[18] It requires that AI systems are built using an ethical methodology that is just and ethically permissible, based on human rights and cultural values, to generate a beneficial effect for individuals and communities. Relevant controls include defining how the AI system will align with fundamental human rights and Saudi Arabia's cultural values, adhering to ethical data management frameworks and processes, properly acquiring data, ensuring AI systems have the appropriate parameters and algorithm training to attain outcomes that advance humanity, and establishing mechanisms for assessing AI systems against fundamental human rights and cultural values.

Principle 5 (see Section IV.ii, below) is also relevant.

ii Quality and performance

Principle 5, on reliability and safety, requires that the AI system adheres to the set specifications and that the AI system behaves as intended.[19] Reliability is described as 'a measure of consistency and provides confidence in how robust a system is' and safety is 'a measure of how the AI system does not pose a risk of harm or danger to society and individuals'. Relevant controls include designing an AI system that can withstand uncertainty and volatility, measuring the data sample's quality, accuracy, suitability and credibility, testing how the system behaves under outlier events and implementing human oversight of high-impact decisions. There is a prohibition on using AI systems for social scoring or mass surveillance purposes.

Principle 4, on social and environmental benefits, requires that AI systems should not 'cause or accelerate harm or otherwise adversely affect human beings but rather contribute to empowering and complementing social and environmental progress'. This incorporates protecting social good and environmental sustainability.[20] Relevant controls include considering social and environmental issues when designing AI systems, ensuring the ultimate goal of models and algorithms is linked to a socially recognised end and ensuring a continuous assessment of the human, social, cultural, economic and environmental effects of AI technologies.

iii Transparency and accountability

Principle 6, on transparency and explainability, requires that AI systems are built with a high level of clarity and explainability, and include features to track automated decision-making.-[21] Data, algorithms, processes and the purpose of the AI system need to be transparent and communicated, as well as being explainable, to those affected. Relevant controls include ensuring stakeholders affected by AI systems are informed of how outcomes are processed and given an explanation of the rationale for the decisions made, including a process mechanism to log and address issues and complaints, documenting the input data sets to allow for traceability and transparency, and to ensure compliance with data privacy regulations and intellectual property standards, carrying out AI ethics due diligence where an AI system is built by a third party and logging information on data breaches.

Principle 7, on accountability and responsibility, holds anyone involved with an AI system 'ethically responsible and liable for the decisions and actions that may result in a risk and negative effects on individuals and communities', even if the adverse effect was not intended.[22] Relevant controls include attributing ethical responsibility and liability for the outcomes of the AI system at the plan and design phase, carrying out necessary data quality checks on input data and cleansing the data of societal bias and sensitive features where possible, and predefining alerts for performance metrics.

iv 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.[23]

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[24] 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.

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'.[25] Saudi Arabia has published a National Intellectual Property Strategy (NIPST),[26] 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 relation to Principle 6, on transparency and explainability, with a requirement for input data to be acquired and collected in adherence with intellectual property standards and controls.[27]

v Liability

The AI Ethics Principles require entities and individuals to adopt certain standards and ethics when developing and using AI-based systems; however no specific penalties are set out for non-compliance with the relevant rules. 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 system; 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[28] 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[29] 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,-[30] 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.

vi 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. Please see the sections above on fairness, bias and discrimination, and transparency and accountability.

vii Disclosure and notice-of-use requirements

See Sections IV.vi and IV.iii.

viii Jurisdiction

The jurisdictional scope of rules relating to the use of technologies is generally broad; for example, the AI Ethics Principles apply to any persons designing, developing, deploying, implementing, using or being affected by AI systems within Saudi Arabia. A similar approach is taken by industry-specific rules, such as the Consumer Protection Law, which was drafted to apply to the relationship between the consumer and the economic operator with regard to any product or service offered or made available in Saudi Arabia. Similarly, the PDPL applies to any processing of personal data by any means that takes place in Saudi Arabia, including any processing of personal data relating to individuals residing in Saudi Arabia, by entities outside Saudi Arabia.[31]

ix Other

Cybersecurity

In Saudi Arabia, cybersecurity is of utmost importance. The National Cybersecurity Authority (NCA) introduced a number of cybersecurity-related requirements, in particular its Essential Cybersecurity Controls (ECCs),[32] which are mandatory for government organisations (including government-owned companies and entities) and private sector organisations who own, operate or host 'critical national infrastructure', and are recommended for other organisations. They require organisations to take various data security measures, including to 'be prepared for handling artificial intelligence'. The NCA's Critical Systems Cybersecurity Controls (CSCC)[33] also impose cybersecurity requirements and apply to any organisation that owns or operates critical systems (i.e., any system or network whose failure, unauthorised change to its operation, unauthorised access to it or to the data stored or processed by it, may result in a negative effect on the availability of the organisation's businesses and services, or cause negative economic, financial, security or social effects at the national level). AI systems could be considered critical systems depending on their use and scope; for example, if an unauthorised change to the model or relevant data could have a negative effect on services provided to a large number of individuals or result in significant financial losses. A key requirement in the CSCC is a prohibition against remote access to systems from outside Saudi Arabia, which applies in addition to data localisation requirements in the ECCs, which prohibit information hosting outside Saudi Arabia.

Data protection

Under Principle 2, on privacy and security,[34] AI systems must be built in a way that respects the privacy of data collected and upholds data security. Relevant controls include: planning and designing the AI system so that there is respect for the privacy of individuals; ensuring 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.[35]

Although not specific to AI, a number of PDPL requirements will affect AI systems 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;[36]
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;[37]
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;[38]
4. sensitive data: a number of categories of personal data are defined as sensitive, and are subject to more stringent data protection 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 is also considered as sensitive under the AI Ethics Principles, but is not sensitive under the PDPL (although additional controls apply to credit data);[39] and
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.[40] 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.

Enforcement

There is no AI-specific enforcement in Saudi Arabia at the time of writing.

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 numbers 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. Further, there is a lack of common standards in information security (particularly in relation to cloud technology) across the various participants in the legal market, which hinders rapid and wide adoption of AI. 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 things are certain with respect to AI and Saudi Arabia: (1) the public and private sectors will make significant investments in AI technology 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) the SDAIA, SAIP and other regulators will issue additional laws and regulations focusing on the development, operation and use of AI technology in Saudi Arabia.

The PDPL entering into force in September 2024 will affect a large number of organisations in Saudi Arabia that use personal data as part of the data set for an AI model.

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.

Endnotes

[1] Brian Meenagh is a partner and Ksenia Koroleva and Lucy Tucker are associates at Latham & Watkins LLP. ^ Back to section

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

[3] https://ai.sa/. ^ Back to section

[4] https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf. ^ Back to section

[5] AI Ethics Principles (Version 1.0), p. 6. ^ Back to section

[6] Personal Data Protection Law (PDPL), available at https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V-2-23April2023-%20Reviewed-.pdf. ^ Back to section

[7] 'The Implementing Regulation of the Personal Data Protection Law', available at https://sdaia.gov.sa/en/SDAIA/about/Documents/ExecutiveRegulations.pdf. ^ Back to section

[8] PDPL, Article 2(1). ^ Back to section

[9] AI Ethics Principles, p. 8. ^ Back to section

[10] id., p. 29. ^ Back to section

[11] id., p. 32. ^ Back to section

[12] id., p. 8. ^ Back to section

[13] id., p. 30. ^ Back to section

[14] id., p. 32. ^ Back to section

[15] id., pp. 34–40. ^ Back to section

[16] id., p. 40. ^ Back to section

[17] id., pp. 12–14. ^ Back to section

[18] id., pp. 17–19. ^ Back to section

[19] id., pp. 21–23. ^ Back to section

[20] id., pp. 19–20. ^ Back to section

[21] id., pp. 23–25. ^ Back to section

[22] id., pp. 25–27. ^ Back to section

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

[24] 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%
1_0.pdf. ^ Back to section

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

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

[27] AI Ethics Principles, p. 24. ^ Back to section

[28] See footnote 23, above. ^ Back to section

[29] 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

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

[31] PDPL, Article 2(1). ^ Back to section

[32] https://nca.gov.sa/ecc-en.pdf. ^ Back to section

[33] https://www.nca.gov.sa/cscc-en.pdf. ^ Back to section

[34] AI Ethics Principles, pp. 15–17. ^ Back to section

[35] id., p. 22. ^ Back to section

[36] PDPL, Articles 11, 14, 18 and 19. ^ Back to section

[37] id., Articles 5 and 6. ^ Back to section

[38] id., Articles 4 and 12, and PDPL Implementing Regulations, Articles 3 to 8. ^ Back to section

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

[40] PDPL, Article 22. ^ Back to section

LATHAM & WATKINS LLP

Brian Meenagh brian.meenagh@lw.com
Ksenia Koroleva ksenia.koroleva@lw.com
Lucy Tucker lucy.tucker@lw.com

Latham & Watkins LLP

Read more from this firm on Lexology