IN-DEPTH

Technology, Media And Telecommunications

SAUDI ARABIA

LEXOLOGY

Technology, Media and Telecommunications

EDITION 16

Contributing Editor

Matthew T Murchison

Latham & Watkins LLP

In-Depth: Technology, Media and Telecommunications (formerly The Technology, Media and Telecommunications Review) provides a practical, business-focused survey of law and policy in the TMT sector across key jurisdictions worldwide. With a focus on recent trends and developments, it also offers useful insights into how this legal and policy landscape continues to evolve from year to year.

Generated: November 10, 2025

Saudi Arabia

Brian Meenagh, **Ksenia Koroleva**, **Danielle van der Merwe**, **Faisal Imam** and **Fady Saleh**

Latham & Watkins LLP

Summary

Introduction

The pace of change and maturation of the regulatory regime for technology, media and telecommunications in the Kingdom of Saudi Arabia is simply breathtaking. This is the sixth annual iteration of this chapter, and every year since the original 2020 edition has required updates to the chapter.

Significant developments have occurred in the areas of content moderation, digital infrastructure, privacy and data protection. The regulatory changes are intended to foster innovation and support the adoption of technologies like artificial intelligence and the internet of things (IoT). There is a notable surge in the use of social media, indicating a growing digital engagement among the population, and driving the introduction of new content creator guidelines reflects the country's commitment to aligning digital content with cultural values and legal standards. There is also a rise in telecom transactions, highlighting the increasing reliance on digital communication and financial services. Furthermore, Saudi Arabia is enhancing its international cooperation, which may foster global partnerships and contribute to the country's Vision 2030 goals of economic diversification and modernisation. The Saudi Data & AI Authority (SDAIA) issued new and amended regulations, guidance and documents for the Personal Data Protection Law (PDPL),[1] such as the updated Transfer Regulations,[2] Standard Contractual Clauses (SCCs)[3] and guidance on Binding Corporate Rules (BCRs).[4] Additionally, SDAIA issued Rules for appointing a Data Protection Officer,[5] and guidelines on privacy policies,[6] data minimisation,[7] data destruction,[8] data disclosure[9] and records of processing activities.-[10]

This chapter covers all of these developments and more – in particular it builds upon the work of previous chapters to provide an up-to-date overview of the key technology, media, telecommunications and data regulations applicable to entities in Saudi Arabia. As in previous years, this chapter cannot claim to be comprehensive, but we have sought to provide the reader with a map to navigate the complex and evolving regulation regime in Saudi Arabia.

Year in review

The main updates have come from SDAIA in the context of data privacy and AI, as follows:

1. SDAIA issued the final updated Transfer Regulations, following a number of amended versions and public consultations over the course of 2024 concerning cross-border transfers of personal data;[11]
2. SDAIA issued SCCs[12] and Guidance on BCRs[13] for cross-border transfers of personal data;
3. SDAIA issued Rules for Appointing a Personal Data Protection Officer[14] and other rules concerning compliance with the PDPL; and
4. there are rules relating to the National Register of Controllers in Saudi Arabia.[15]

The PDPL came into force as of 14 September 2024. This has been long awaited by local and international entities that operate from Saudi Arabia or process the personal data of individuals located in Saudi Arabia: the publication of the final versions of both the PDPL[16] and the Implementing Regulations[17] (including the Transfer Regulations and related SCCs and BCRs) means that entities should now ensure that they have taken appropriate steps to comply with the new law.

Regulation

The regulators

The technology and telecommunications sector in Saudi Arabia is principally regulated by two bodies: the Ministry of Communication and Information Technology (MCIT)[18] and the Communication, Space and Technology Commission (CST).[19]

Other authorities have more discrete remits. For example, the National Cybersecurity Authority (NCA)[20] has regulatory and operational functions pertaining to cybersecurity, enjoys financial and administrative independence and reports to the King directly. The NCA is entitled to have affiliate centres to carry out some of its responsibilities and tasks, including the Saudi Computer Emergency Response Team (CERT), originally operating under the auspices of CST but transferred to the NCA by the Royal Decree establishing the NCA.[21]

The key regulators for media and media protection in Saudi Arabia are the Ministry of Media (MoM),[22] the General Authority of Media Regulation (GAMR)[23] and the Digital Content Council.[24] The General Commission of Audiovisual Media (GCAM)[25] was previously responsible for audiovisual media; however, in September 2023, GCAM was replaced by GAMR, with GAMR having supervisory jurisdiction over all forms of media. In December 2023, GAMR launched its strategy with the aim of positioning Saudi Arabia's media sector as a regional and international leader, enhancing its investment attractiveness and improving the efficiency of its national workforce.[26] GAMR's strategy also targets increasing the media sector's contribution to the gross domestic product of Saudi Arabia to 47 billion riyals by 2030, leveraging the sector's opportunities to diversify the national economy and boost non-oil gross domestic product.

Further details on each regulator are set out below.

Technology and telecommunications

Key regulators

The MCIT is responsible for making general policies and development programmes and representing Saudi Arabia in domestic, regional and international bodies in the technology and telecommunications sector. The MCIT oversees the implementation of several laws, including the Telecommunications and Information Technology Act (issued by Royal Decree No. (M/106), dated 02/11/1443H (corresponding to 1 June 2022)) (the Telecoms and IT Act).

The CST is responsible for issuing licences in accordance with the Telecoms and IT Act and implementing approved plans and programmes for the supervision and management of the technology and telecommunications sector. The CST issued various regulations and guidelines on the provision of digital infrastructure services, including a regulation on mobile towers and network sharing rules,[27] a set of guidelines on disaster recovery planning applicable to data centres,[28] regulations on the registration of satellites and the provision of telecommunication services over satellites,[29] and the Regulations for Establishing and Providing Telecommunications Services in Real Estate,[30] which set requirements for property owners and developers to ensure early, code-compliant installation of telecom infrastructure. Additionally, the CST issued a public consultation on a draft Global AI Hub Law in April 2025, which aims to establish three types of AI hubs and introduce 'data embassies' for foreign entities' data.

Other relevant regulators

SDAIA and its sub-entities – the National Data Management Office (NDMO), the National Information Center (NIC) and the National Center for AI (NCAI) – work on providing a data-driven and AI-supported government and economy, and to own the national data and AI agenda to help achieve Vision 2030's goals.[31]

SDAIA aims to supervise the implementation of the PDPL for two years after its implementation, following which a transfer of supervision to the NDMO will be considered.[32]

The National Centre for Digital Certification (NCDC) was established in 2001 and transferred to the remit of the MCIT for management in 2005. The NCDC is primarily responsible for the management of public key infrastructure (i.e., a set of roles, policies and procedures needed to create, manage and distribute digital certificates and manage public key encryption).[33] As of February 2025, Saudi Arabia has shifted the issuance of conformity certificates for telecommunications products from the CST to the SABER,[34] an electronic certification platform.

The National Digital Transformation Unit (NDTU) was established in 2017 and aims to develop and further the digitisation of citizen services in partnership with the private sector. A notable example of this in 2017 was the setting up of FekraTech, an interactive platform that enables citizens to participate in Saudi Arabia's national digital transformation by submitting digital solutions to existing challenges; the NDTU worked alongside the Ministry of Health for the initiative's initial project, whereby individuals proposed solutions to a number of health-related issues.[35]

The Saudi Authority for Intellectual Property (SAIP) was established in 2018 with the aim of organising, supporting, sponsoring, protecting and promoting intellectual property in Saudi Arabia in accordance with global best practices.[36]

Cybersecurity regulators

The Ministry of Interior (MOI) oversees numerous bodies that work to maintain Saudi Arabia's security and manage its internal affairs. Its objectives and responsibilities include:

1.

achieving security and stability, providing safety for Saudi Arabia citizens and protecting against crime;

2. reinforcing security relationships with neighbouring Arab and Gulf Cooperation Council countries, maintaining safety in Saudi Arabia and abroad, controlling crime and drug smuggling and exchanging security information; and
3. reinforcing security cooperation with neighbouring countries to protect cultural possessions and achievements, supporting internal and external security, controlling crime, terrorism and drug smuggling and developing Arab security institutions.

In addition to the above responsibilities, all cybercrimes must be reported to the MOI.[37] Prosecutions are led by the Bureau of Investigation and Prosecution.[38]

The NCA was established by royal decree in 2017 as the body responsible for the protection and promotion of cybersecurity matters in Saudi Arabia. In 2017, it issued a set of minimum standards to be applied by various national agencies to reduce the risk of cyber threats; these controls considered governance, strengthening cybersecurity, enhancing external cybersecurity, cloud computing and industrial control systems and ultimately became consolidated in the NCA's Essential Cybersecurity Controls (ECC – 1: 2018)[39] and Cloud Cybersecurity Controls (CCC – 1: 2020).[40] In 2024, the NCA issued the Cybersecurity Guidelines for Internet of Things (CGIoT-1:2024),[41] which provide a framework for best practices that are recommended to be applied in all organisations that utilise internet of things (IoT) technologies across Saudi Arabia's IoT landscape, as well as cybersecurity principles in manufacturers' products and services, with the objective of reducing cybersecurity risks.

The NCA has both regulatory and operational functions related to cybersecurity. It works closely with public and private entities to improve the cybersecurity posture of Saudi Arabia to safeguard its vital interests, national security, critical infrastructure, high-priority sectors and government services and activities in alignment with Vision 2030. From 2022, any entities providing cybersecurity solutions, services or products in Saudi Arabia have to be registered with the NCA. The NCA is conducting cyber assessments, including compliance assessments and technical cyber assessments of sensitive systems, to monitor cyber risks at the national level and measure the level of compliance with the requirements and controls issued by the NCA.[42]

In September 2025, the NCA released its Report on 'Key Economic Indicators in the Cybersecurity Sector in the Kingdom 2025'.[43] It highlights the market's size, its contribution to GDP, and workforce metrics, reflecting the sector's expansion. In 2024, the cybersecurity market reached 15.2 billion riyals, with government and private sectors contributing significantly to this expenditure. Additionally, a comprehensive classification of cybersecurity products and services was developed, encompassing five main categories, 26 detailed activities and 102 products and services, aligning with global best practices.

The NCA also oversees the activities of other centres and entities, including Saudi CERT, whose primary mission is to raise cybersecurity awareness in Saudi Arabia.[44] In 2022, the NCA launched the National Portal for Cyber Security Services (HASEEN) to develop cybersecurity-related services and improve cybersecurity in Saudi Arabia.[45] In February

2025, the NCA also launched the National Program for Research, Development, and Innovation (RDI)[46] in cybersecurity to enhance the cybersecurity landscape in Saudi Arabia by fostering research and innovative solutions for current and future challenges. The program, developed in collaboration with the Saudi Information Technology Company (SITE), introduces three initiatives — 'Cyber Research and Innovation Pioneer Grants', 'Cyber Industry Research Grants' and 'Cyber Innovation Bridges' — targeting universities, research institutions and experts, and focusing on eight key areas, including NextGen Cyber Defense and AI x Cyber. In October 2025, the fifth Global Cybersecurity Forum in Riyadh announced, through the NCA, certain major initiatives, including the establishment of the Centre for Cyber Economics with the World Economic Forum, to enhance global cyber resilience and economic stability through research and collaboration. The forum also launched initiatives like the Child Protection and Cyberspace Initiative and focused on bridging the gender gap in cybersecurity, aiming to create a secure, inclusive cyberspace that supports economic growth and societal prosperity.[47]

Further, the NCA expanded and updated its comprehensive 'Cybersecurity Toolkit' to enhance cyber preparedness across public and private sectors. The new tools, accessible in both Arabic and English on the NCA website, include updated models, policies, standards and procedures designed to strengthen cybersecurity measures. Developed through rigorous analysis and adaptation of global best practices, the Toolkit covers various topics such as cybersecurity responsibilities, strategy formulation, malware protection, email and network security, web application protection, user device security and more. This initiative aims to foster a cyber-conscious environment and reduce cyber risks in Saudi Arabia.[48]

Media

The MoM is the governmental body tasked with the regulation of Saudi Arabia's media and communications with other countries.

In September 2023, GAMR replaced GCAM, and GAMR now has supervisory jurisdiction over all forms of media, under Cabinet Decision No. 174 dated 27/2/1445H (corresponding to 12 September 2023) (the GAMR Regulations). Under the GAMR Regulations, GAMR regulates the media sector in Saudi Arabia, including broadcasting activities, setting controls for media content and regulating the status of media workers, and to fulfil these objectives, GAMR may carry out activities such as developing media policies, proposing media laws and regulations, determining licence fees for media activities, setting technical specifications for equipment, monitoring service providers in the media sector, regulating advertising activities and regulating digital content. GAMR reports to the MoM but is a separate legal entity with independent finance and administration. However, there is little information available to date on GAMR and online links still refer to the GCAM website. Prior to the 2023 announcement, GCAM was responsible for the regulation of audiovisual media transmission in Saudi Arabia.

The Digital Content Council was established in September 2021 by the MCIT, the Ministry of Information, the Ministry of Culture, the Ministry of Commerce, the Ministry of Investment, the CST, GCAM and SAIP and aims to encourage development of and investment into the digital content sector.[49]

Main sources of law

Technology and telecommunications

The main sources of technology and telecommunications law are as follows:

1. the Telecom Act (issued under the Council of Ministers Resolution No. (74), dated 05/03/1422H (corresponding to 27 May 2001), and approved pursuant to the Royal Decree No. (M/12), dated 12/03/1422H (corresponding to 3 June 2001)) was repealed and replaced with the Telecoms and IT Act on 7 December 2022, which has a broader scope, covering not just telecommunication services but also ICT activities and services, and aims to facilitate the development of Saudi Arabia's digital infrastructure;[50]
2. the Communication and Information Technology Commission Ordinance (the CST Ordinance) (issued under the Council of Ministers resolution No. (74), dated 05/03/1422H (corresponding to 27 May 2001), and amended pursuant to the Council of Ministers resolution No. (133), dated 21/05/1424H (corresponding to 21 July 2003));[51] and
3. the E-Commerce Law 2019 (Royal Decree No. M/126 dated 07/11/1440H (corresponding to 10 July 2019)).[52]

The CST's role expanded beyond telecommunications (such as becoming the regulator and oversight entity over civil space matters), and it issued a variety of implementing regulations and consultations[53] in a number of sectors in the technology and digital space, including:

1. the Regulations for Cybersecurity Operations in ICT & Postal Sector (version 1, issued in August 2022), which establishes the ICT-CSIRT which is responsible for promoting cybersecurity across the ICT and postal sector;[54]
2. the Regulations for Providing Digital Content Platform Services (dated October 2023), with the deadline for compliance falling on 8 October 2024;[55]
3. the draft Competition Regulations for Digital Content Platforms issued in July 2022, which was subject to a public consultation period ending 11 September 2022 and which regulates competition between digital content platforms in Saudi Arabia;[56]
4. the Data Centres Regulation issued in August 2023, which imposes minimum service standards for entities providing data centre services in Saudi Arabia, categorises different tiers for data centres and imposes liability on such entities for any losses caused by their negligence;[57]
5. the Net Neutrality Regulations (version 1, issued on 18 July 2023), which protects users' rights to freely access and distribute information regardless of the terminal device used or the origin or destination of the information and requires service providers to treat all internet access services traffic equally;[58]
6. the Cloud Computing Services Provisioning Regulations (version 4, which came into effect on 23/03/1445H (corresponding to 8 October 2023)),[59] which replace the previous Cloud Computing Regulatory Framework (version 3). The Cloud Computing Services Provisioning Regulations outline the obligations and rights

of each of the cloud computing service providers and the cloud customers (subscribers) and apply to cloud computing services provided to customers (subscribers) in Saudi Arabia and to cloud data centres in Saudi Arabia. They oblige cloud service providers to register with the CST in certain cases. The Cloud Computing Services Provisioning Regulations aim to develop the communications and information technology sector in order to stimulate investment in cloud computing in Saudi Arabia and enhance competition in the cloud computing market;

7. the Regulations for Providing Electronic Aggregation in Telecommunications Services (version 1, which came into effect on 23/03/1445H (corresponding to 8 October 2023)), which aim to enable investment in telecommunication services and devices by incentivising trusted telecommunication services;[60]
8. the Regulation for the Reduction of Spam (the Spam Regulations), which requires telecommunications service providers to reduce spam messages transmitted across their networks, including by implementing prevention and monitoring mechanisms. Spam messages are defined as certain types of electronic messages sent without any opt-out mechanism;[61]
9. the Internet of Things Regulatory Framework, issued in September 2019 and further updated in 2024, when it was renamed the 'IoT Regulations';[62]
10. Rules and Conditions for MVNO Services and IoT-VNO Services Provision, which update the conditions and licensing requirements for the request of a licence to provide mobile virtual network operator services. They set out the conditions and licensing requirements for the provision of the services by internet of things virtual network operators;[63]
11. the Saudi Domain Name Registration Regulation[64] and related guidelines and rules;[65]
12. the regulations, guidelines and rules for the registration of Saudi country-code top-level domains, which are issued by the Saudi Network Information Centre (SaudiNIC),[66] part of the CST;
13. the Rules and Technical Standards for ICT Infrastructure Deployment in New Developments, which are intended to facilitate the implementation and rollout of telecoms networks;[67] and
14. the Frequency Spectrum Regulations for Radio Services and Applications regulating the use of the radio frequency spectrum.[68]

Additional regulatory documents issued by the CST concerning the technology and telecoms sector can be found on the CST website.[69]

Cybersecurity

The key relevant cybersecurity laws are as follows:

1. Royal Decree No. 5/11/8697 dated 26/8/1370H (corresponding to 2 June 1951) (the Law Establishing the Ministry of Interior);
2.

the Anti-Cyber Crime Law (issued under the Council of Ministers Decision No. 79, dated 7/3/1428H (corresponding to 26 March 2007), and approved by Royal Decree No. M/17, dated 8/3/1428H (corresponding to 27 March 2007)) (the Cyber Law);[70] and

3. the Cloud Computing Services Provisioning Regulations.[71]

The NCA issued a number of cybersecurity controls, including the Essential Cybersecurity Controls (ECC)[72] and the Cloud Cybersecurity Controls (CCC).[73] The ECC apply to all government organisations in Saudi Arabia, as well as to private sector organisations owning, operating or hosting critical national infrastructure. The CCC apply to any cloud service provider that is providing services to cloud service tenants who are within the scope of the ECC. There are also Critical Systems Cybersecurity Controls, which have a similar scope as the ECC but are focused on critical systems. In late 2024, the NCA conducted a public consultation on the updated ECC (ECC-2) from 30 September to 15 October,[74] and subsequently issued the final version in October 2024.[75] The ECC-2 represent a significant update to the Kingdom's cybersecurity framework, introducing changes to scope, data localisation, Saudisation requirements and streamlining of controls.

In March 2024, the NCA issued the National Policy for Managed Security Operations Centers (MSOC) and a Regulatory Framework for Licensing MSOC Services. These measures are intended to enhance cybersecurity situational awareness at both the organisational and national levels, ensure access to high-quality and reliable MSOC services, and stimulate growth and innovation in the Kingdom's cybersecurity sector. The framework sets out requirements for MSOC service providers serving government entities, critical infrastructure, and other organisations, with the aim of encouraging investment and developing national capabilities.[76]

In August 2025, the NCA released the National Framework for Cybersecurity Risk Management (NFCRM-1:2025), aiming to unify and enhance cybersecurity risk practices across the Kingdom by providing a structured methodology for risk identification, assessment and management. A key mandate includes appointing a Cybersecurity Liaison Officer to ensure compliance and coordination with the NCA, reflecting a national focus on governance, accountability and centralised cybersecurity risk management.

In August 2022, the CST also issued Regulations for Cybersecurity Operations in the ICT and Postal Sector.[77] In 2024, the NCA issued the Cybersecurity Guidelines for Internet of Things (CGIoT-1:2024).

On 14 April 2023, Saudi Arabia announced the launch of four new special economic zones (SEZs) under the supervision of the Economic Cities and Special Zones Authority (ECZA). These SEZs aim to enhance the country's global competitiveness by providing an investor-friendly regulatory environment, competitive sector-specific incentives, and integrated government services. The new SEZs – King Abdullah Economic City (KAEC) SEZ, Ras Al-Khair SEZ, Jazan SEZ and Cloud Computing SEZ – focus on key growth sectors, including cloud computing. This initiative aligns with Saudi Vision 2030 and aims to attract foreign direct investment and global talent, and foster economic development.

Each SEZ offers unique advantages in the relevant areas, for example, Cloud Computing SEZ, driven by the National Strategy for Digital Transformation, supports cloud computing services across multiple locations in Saudi Arabia.[78]

There are also a number of sector-specific cybersecurity rules and requirements, for example, for the finance sector, the SAMA Cyber-Security Framework (version 1, May 2017)[79] and the Cybersecurity Guidelines for Capital Markets Institutions, issued by the Capital Markets Authority.[80]

Privacy

In September 2021, the PDPL was issued (pursuant to Cabinet Resolution No. 98 of 7/2/1443H and Royal Decree M/19 of 9/2/1443H). In March 2023, the PDPL was amended (pursuant to Royal Decree No. M/148 of 05/09/1444H).[81] The PDPL delegates a lot of matters to the Implementing Regulations, the final version of which was issued by SDAIA in September 2023, following a public consultation.[82] The Implementing Regulations also contain Implementing Regulations on personal data transfers outside Saudi Arabia. The PDPL came into force on 14 September 2023, with a one-year compliance transition period, which ended on 14 September 2024.

In 2024, SDAIA issued a comprehensive set of new regulations, guidance, and documents related to the PDPL. These include the final updated Transfer Regulations, SCCs,[83] and BCRs[84] for data transfers outside Saudi Arabia. Additionally, SDAIA introduced Rules for Appointing a Personal Data Protection Officer (DPO), Rules Governing the National Register of Controllers within the Kingdom and guidelines on privacy policies, data minimisation, data destruction, data disclosure, data sharing, records of processing activities, personal data breach incidents, binding corporate rules and standard contractual clauses. In April 2025, SDAIA issued a public consultation on certain proposed amendments to the Implementation Regulations which, amongst other key updates, seek to consolidate and clarify the responsibility of the DPO role and also seek to repeal the standalone DPO Rules. The consultation ended in May 2025 and the outcome is awaited.[85]

Telecommunications service providers are also subject to data protection requirements under the Telecoms and IT Act.

There are also criminal offences for privacy violations in the Cyber Law.

In line with its commitment to fostering responsible innovation in personal data protection, SDAIA has launched the 2025 Regulatory Sandbox Program. This regulatory testing initiative enables Saudi-registered startups and SMEs to trial innovative digital solutions involving the processing of personal data in accordance with the PDPL. The program provides a controlled environment in which participants with a working prototype may experiment with new services that require regulatory flexibility. The initiative is designed to promote responsible innovation while ensuring alignment with both local and international privacy standards.[86]

Media

The key laws regulating media and media protection are as follows:

1. the Publications Law promulgated by Royal Decree No. M/32 dated 03/09/1421H (corresponding to 29 November 2000), and its implementing regulations issued pursuant to a resolution of the Minister of Media dated 16/06/1422H (corresponding to 4 September 2001), as amended;

2. the Electronic Publications Regulations published on 20/04/1432H (corresponding to 25 March 2011);
3. the Press Institutions Law promulgated by Royal Decree No. M/20 dated 08/05/1422H (corresponding to 29 July 2001);
4. the Audiovisual Media Regulations promulgated by Royal Decree number 33/M dated 25/03/1439H (corresponding to 13 December 2017) with additional rules adopted in 2024 to further emphasise adherence to principles of objectivity, honesty, accuracy, confidentiality and fairness in media and content restrictions;
5. the GAMR Regulations; and
6. the Copyright Law promulgated by Royal Decree No. M/41 dated 02/07/1424H (corresponding to 30 August 2003).

As described under 'Media', above, GAMR replaced GCAM as regulator in the media sector and issued a number of regulations particularly geared towards regulating audiovisual content, setting age requirements and licensing procedures for this category of content. The regulations issued have not touched upon written publication nor superseded the Publications Law as was previously expected. On 5 November 2023, GAMR launched a public consultation for its draft Media Law. The document aims to overhaul Saudi Arabia's media regulatory framework by replacing the Audiovisual Media Regulations and the Publications Law. It seeks to strengthen the end-to-end regulatory role, define an investor-friendly regulatory approach and support sector growth to enhance media revenue and GDP. It also aims to provide clarity on content development within the Saudi context, safeguard the audience, foster trust in media and adapt to recent developments in media, technology and consumer trends.

In September 2025, GAMR introduced new content regulations for all media platforms, focusing on protecting privacy and social values. The regulations prohibit inappropriate language, ostentatious displays, filming of children or domestic workers, invasion of privacy, bullying, unauthorised filming, revealing attire and misleading information. Violations of these guidelines, which aim to protect children and uphold national identity, will result in regulatory action, emphasising modesty and the safeguarding of social values.[87]

In a further step towards enhancing the regulatory environment for digital content, the Saudi Broadcasting Authority (SBA) has initiated a public survey to solicit feedback from the business sector and relevant stakeholders on proposed amendments to the Digital Content Production and Management Regulations. This initiative seeks to engage stakeholders in reviewing and updating key provisions to enhance transparency, align with evolving digital practices, and strengthen protections for both clients and service providers in the digital content sector.[88]

Publications and press institutions

For the implementation of media laws in relation to publications, the MoM applies:

1. the Publication Law and its implementing regulations, regulating print and publication activities; and

2. the Implementing Regulations for Electronic Publishing, regulating the practice of electronic publishing in Saudi Arabia.

Audiovisuals

For the implementation of media laws applicable to audiovisuals, GAMR issued the implementing regulations to the Audiovisual Media Regulations[89] governing the following matters:

1. importing and selling receivers;
2. licensing visual and audible media content production companies;
3. establishing a representative office of TV channels;
4. importing, distributing, selling and renting visual and audible media content;
5. establishing studios;
6. audiovisual broadcasting services over telecommunication networks;
7. TV and radio competitions;
8. satellite news gathering services;
9. audio social communication services;
10. visual broadcasting via closed circuit services;
11. on-demand video services; and
12. videogame participation.

Digital content platforms

The CST issued the Regulations for Providing Digital Content Platform Services (dated October 2023) (Digital Platform Regulations), with the deadline for compliance falling on 8 October 2024.[90]

The Digital Platform Regulations aim to regulate service providers' activities specifically in the following sectors:

1. digital video platforms, including satellite pay TV platforms, IPTV platforms, video over-the-top (OTT) platforms and video sharing platforms;
2. digital audio platforms, including audio-on-demand platforms and internet radio platforms;
3. digital gaming platforms, including online gaming platforms and e-sports participation platforms;
4. digital advertising platforms, including online advertising platforms and social media platforms; and
5. any other digital content platforms that CST deems to be included in the scope of the regulations in the future, within the definition of 'digital content platform'.

The Digital Platform Regulations apply to video, audio, gaming and marketing digital platforms that provide services to users in Saudi Arabia and include obligations to obtain regulatory tools depending on the service classification.[91]

In addition, the CST introduced a draft of Competition Regulations for Digital Content Platforms for public consultation in July of 2022, which have not yet been published in their final form. The Competition Regulations for Digital Content Platform seek to establish competition principles between digital content platform services providers regulated by the Digital Platform Regulations.

In September 2023, the CST issued a consultation on a Global Digital Content Safe Harbour Law[92] which aims to support Saudi Arabia's transformation into a highly competitive digital hub, by exempting pre-qualified intermediary services from liability for providing services that include global digital content that violates Saudi Arabia's laws. Intermediary services are services that host, store or otherwise process global digital content outside Saudi Arabia or that enable access to this content. The draft Global Digital Content Safe Harbour Law contains requirements for pre-qualification with CST in order to benefit from the safe harbour and sets out possible penalties for noncompliance with the safe harbour regime, which include fines of up to 25 million riyals.

Regulated activities

Technology

The Telecom Act and the newly introduced Telecoms and IT Act[93] provide a legal foundation for supervising and managing the telecommunications sector in Saudi Arabia. The Telecom Act outlined certain objectives for the sector. These included:

1. providing advanced and adequate telecommunications services at affordable prices;
2. ensuring the provision of access to the public telecommunications networks, equipment and services at affordable prices;
3. ensuring the creation of a favourable atmosphere to promote and encourage fair competition in all fields of telecommunications;
4. safeguarding the public interest and user interest as well as maintaining the confidentiality and security of telecommunications information; and
5. ensuring the transfer and migration of telecommunications technology to keep pace with its development.

The Telecoms and IT Act replaces the conflicting provisions of the Telecom Act, built on and expanded these objectives and aimed to enhance the sector in a number of ways to increase its robustness and build trust in it. A few of the objectives listed under the Telecoms and IT Act are:

1. encouraging the sector in a way conducive to expanding and improving its services and infrastructure;

2. encouraging digital transformation and the move towards digitising services;
3. encouraging innovation and entrepreneurship in the sector; and
4. protecting public interest and the privacy of the user and increasing the level of trust in dealings within the sector generally.

Any entity seeking to provide telecommunications services or telecommunications and information technology services, including digital content platforms, must submit a licence application to the CST.

The CST Ordinance[94] establishes the CST as the regulatory authority for all matters in the telecommunications sector in Saudi Arabia. It includes reference to the CST's responsibilities, board composition and membership, governance and sources of finance.

The CST is responsible for a wide variety of roles, including:

1. issuing the necessary licences in accordance with all relevant laws;
2. ensuring the implementation of the conditions specified in these licences;
3. implementing approved policies, plans and programmes for developing the telecommunications sector;
4. achieving the orderly expansion of the telecommunications infrastructure and telecommunications services provided to the users in an effective and reliable manner; and
5. encouraging reliance on market forces for the provision of telecommunication services.

Digital content platforms

See above under 'Digital content platforms'.

Cybersecurity

Cloud Service Providers that exercise direct or effective control over data centres or critical cloud infrastructure hosted in Saudi Arabia are required to register with the CST.

Entities providing cybersecurity services, solutions or products in Saudi Arabia must register with the NCA.[95]

Privacy

Under Article 30(4)(c) of the PDPL, the competent authority may establish a national register of controllers, and under Article 34 of the Implementing Regulations to the PDPL, the competent authority shall issue rules for controller registration in the national register.

SDAIA has issued its Rules Governing the National Register of Controllers Within the Kingdom,[96] which provides that data controllers must register on the National Data Governance Platform if they are public entities, their main activity is based on personal

data processing or they process sensitive data. Individuals must register if they process personal data beyond personal or family use.

Media

Publications

Pursuant to the Publications Law, it is necessary to obtain a licence from the MoM to:

1. print, publish or distribute publications or engage in any other publication services;
2. import, sell or rent movies or video tapes;
3. produce, sell or rent computer programs;
4. engage in any press services; and
5. carry out photography services.

These activities are restricted to Saudi nationals. In addition, the holder of a licence may transfer, lease or share ownership of such licence after obtaining the approval of the MoM. Furthermore, the Electronic Publications Regulations stipulates that it is required to obtain a licence from the MoM to carry out electronic publication. This licence is also restricted to Saudi nationals.

The author, publisher, printer or distributor must obtain the MoM's approval prior to circulating a publication. The MoM will not approve a publication that prejudices Islam, the Saudi regime, the interests of the country or public morals and customs.

Press institutions

The Press Institutions Law stipulates that to establish a press institution that carries out the business of publishing magazines and newspapers, an application shall be submitted by the founders of the institution accompanied with the details of the business and the founders to the MoM. The number of founders shall not be less than 30 and all must be Saudi nationals.

The Minister of Media and Information can only grant a licence after the approval of the Council of Ministers. Both the general manager and chief editor of the press institution must be Saudi nationals. The headquarters of the press institution shall be in the city specified by the licence. Some of its publications may be issued in other cities pursuant to approval of the MoM.

Audiovisuals

In order to obtain, renew or cancel a licence from GAMR, the approval of the Council of Ministers may be required.

There are several types of licences that can be obtained from GAMR under the Audiovisual Media Law and its Implementing Regulations, including audiovisual content production licences, printing licences and importing and distributing media content licences. GAMR

may also issue non-objection certificates for a certain set of activities that require this type of limited licence, including establishment of movie theatres, conducting a TV or radio competition and public presentations of media content, among others.

Ownership and market access restrictions

Typically, only those activities listed in the Ministry of Investment (MISA) negative list are prohibited for foreign investors. The MISA negative list is narrow and does not touch upon any of the activities listed in this chapter. Over the past few years, Saudi Arabia has been gradually reducing the number of sectors on the negative list to attract more foreign investment as part of its Vision 2030 initiative. This includes opening up sectors such as retail, wholesale and certain professional services to greater foreign participation. Moreover, the establishment of SEZs with more liberal investment regulations has been a significant development. These zones often have their own set of rules and may offer more relaxed restrictions compared to the national negative list.

However, each regulator has broad discretion when it comes to issuing their licences. Separate from the MISA negative list, each regulator may apply foreign ownership restrictions whether based on its own regulatory framework, policies, security concerns, other interests or solely at its discretion.

At the same time, in September 2025, the MISA launched the 'Saudi Program for Entrepreneurial Companies' to support the establishment and expansion of entrepreneurial companies within the Kingdom. The program provides comprehensive support, including company formation services, strategic networking, and tailored incentives, targeting entrepreneurs, innovators and venture capitalists to position Saudi Arabia as a regional hub for innovation. Key focus areas include healthtech, fintech, AI, biotech and more, with the program adopting global best practices and forming international partnerships to aid Saudi startups.[97]

Transfers of control and assignments

Any merger or acquisition transaction shall be subject to the antitrust regime of Saudi Arabia, as implemented by the General Authority for Competition.[98] From an operational perspective and depending on the type of licence, the requirements for licences transfers may be no action required, notification to the relevant regulator, or obtaining regulator consent (including re-application). The General Authority for Competition issued a guide to economic concentration aimed at aiding the investor to navigate whether the type of economic concentration pursued requires prior approval by the General Authority for Competition.[99]

Furthermore, in 2018 the CST introduced the Procedural Rules for Mergers and Acquisitions in Communications and Information Technology Sector,[100] which provides that the following are considered reviewable transactions subject to the CST's approval or non-objection:

1. mergers between a telecommunications provider licensed by the CST and any other service provider whether inside or outside Saudi Arabia;
2.

an acquisition of 5 per cent or more of the shares or interests of a service provider licensed to operate in Saudi Arabia; and

3. an acquisition of a percentage of shares or interests of a service provider licensed to operate in Saudi Arabia, leading to the monopolisation of a specific telecommunications market by one service provider.

Telecommunications and internet access

Internet and internet protocol regulation

The regulation and classification of internet and IP-based services are governed by the same authorities and pursuant to the same broader set of legislation governing the telecommunications sector in Saudi Arabia. The telecommunications sector may also be subject to other related governmental authorities, each pursuant to its authorities as a regulator. For example, the Ministry of Human Resources and Social Development (MHRSD) has implemented a ministerial decision that was announced on 5 October 2020 and came into effect on 27 June 2021 for Saudisation of a number of occupations within the telecommunications field.[101] The MHRSD frequently updates and expands its Saudisation policies to cover additional sectors and occupations. Therefore, it remains essential to stay informed about any new announcements.

Additionally, there are specific regulations targeting internet and IP-based services in place; for example, see the references in the above sections to the E-Commerce Law, and Cloud Computing Services Provisioning Regulations as well as the various regulations issued by the CST and referred to above.

Universal service

Saudi Arabia encourages the development of telecoms and broadband infrastructure and adopted this under its Vision 2030. Prior to the strategies adopted under Vision 2030, the CST issued the Universal Access and Universal Service Policy[102] (the Policy) in July 2007, which aims to enable 100 per cent of the population to obtain, at a minimum, 'public access to a defined ICT service at a defined quality through reasonably available and affordable public or community facilities' and to subscribe to and use a defined ICT service at a defined quality on an individual or household basis.[103] According to the CST, the Universal Service Fund, the fund established for purposes of achieving the goals of the Policy, has completed projects in 13 regions in Saudi Arabia as of June 2016, resulting in 17,529 served centres, villages and underdeveloped areas.[104] While the core principles of the Universal Access and Universal Service Policy remain consistent, there have been practical enhancements to the policy to address emerging technologies and changing market conditions. For example, recent initiatives focus on expanding broadband access, promoting 5G deployment and enhancing digital literacy.

Restrictions on the provision of service

Service providers are regulated under the Telecoms and IT Act.

In addition, the CST revised its relevant regulations concerning the rights, obligations and terms of ICT service providers and users (the Amended Service Providers Regulations)[105] issued in 2020, and the SPAM Regulations (see above), which aim to reduce unsolicited calls and messages. Both sets of regulations apply to all service providers licensed by the CST and any users thereof.

Under the Amended Service Providers Regulations, service providers must publish clear and transparent information in respect of the terms and conditions of the services being provided or advertised. This information must include the following at a minimum:

1. clarifications about the method of subscription and cancellation mechanisms;
2. types of calls available in the package being purchased or advertised;
3. the number of minutes granted for each type of call available in the package;
4. types of calls excluded from the package;
5. the mechanism for dealing with minutes, data amount or remaining balance;
6. the validity or expiry of remaining balance;
7. an explanation as to the number of minutes or amount of data available, or both, and information about use during or outside peak periods;
8. penalty conditions, if any;
9. provision of the service in the event of implementation of restrictions on use in terms of quality and availability;
10. cases in which usage restrictions apply;
11. any limitations or restrictions on usage that would affect use of the service;
12. necessary means for users to enable them to follow up on their usage; and
13. information concerning the mechanism for applying a settlement with the user where the service provider is unable to meet the quality standards approved by the CST or stipulated in the contract.

Furthermore, the Amended Service Providers Regulations prohibit telemarketing of services or products for purposes of sales without the user's prior consent. Permitted telemarketing must be in accordance with the following:

1. contact must be through official communication channels only;
2. communication must be recorded;
3. the user's identity must be verified;
4. the service provider must disclose the representative's and service provider's names, and verify whether the user has consented to continue the call, at the beginning of the call; and
5. the service provider must explain the offered services in full, disclose the full price of the service and document any request for the offered service.

With respect to contracting, the Amended Service Providers Regulations have stated a number of provisions that must be clearly written in Arabic and English in the service contract, including the identification information of the user, information on the requested service, the starting date of the contract, details of any tariffs or charges required for the services, details of the service, products and their features and details of the terms and obligations, in addition to a number of other standard provisions. Service providers must also ensure that the applicant is at least 15 years old. The service provider may not set a minimum duration for contracting or make any amendments to the contract that are not in the user's interests, without first having obtained the consent of the CST.

In addition, the Amended Service Providers Regulations state service providers may not impose any fees or charges on a service package or offer after a free trial period unless: (1) the user was provided with a notice of the expiry date at least 24 hours in advance; and (2) the user provided a written request for the continuation of the service after the end of the free trial period. Each service provider must also provide free and easy channels for communication between itself and users, offer its services to any users applying for the services and offer each service in a consistent manner to all users. This includes maintaining the same prices for services offered, quality of service, time during which the services are offered and any other conditions imposed by the CST.

Under the Amended Service Providers Regulations, all user information is considered confidential and service providers are obliged to maintain this confidentiality and seek all measures for the purposes of securing user information and prohibiting access, publication, sharing or use thereof. Service providers are also prohibited from disclosing user information unless the disclosure is mandated under another applicable law, is based on the user's consent or is provided based on a request from the CST. Furthermore, the same level of data security must be mirrored in the internal policies of service providers and monitored accordingly.

Service providers are also obligated to maintain the confidentiality of user phone calls and any information transmitted to and from the user or information received through one of the service providers' public networks. They must also prohibit access to this information by any employee or affiliate.

The Amended Service Providers Regulations also contain provisions in respect of invoicing, prepaid services, international roaming services, number portability, assignment of service and suspension of service, in addition to provisions relating to users with disabilities and governmental and business users.

Privacy and data security

The PDPL applies to any processing of personal data by any means that takes place in Saudi Arabia, including any processing of personal data of individuals residing in Saudi Arabia by entities outside of Saudi Arabia.[106] This scope is wide and means that both entities inside Saudi Arabia, and entities located outside Saudi Arabia that are processing the personal data of individuals in Saudi Arabia, will be within the scope of the new PDPL.

The PDPL appears to have been influenced by international data protection regimes including the GDPR; however, there are some areas of divergence. Key legal requirements to note include:

1. under Articles 5 and 6, the consent of an individual is required for processing their personal data, unless an alternative legal basis exists, such as contractual necessity or the legitimate interests of the controller;
2. under Articles 12 and 13, a controller must provide individuals with a privacy notice with information on the personal data processing;
3. under Article 20 of the PDPL and Article 24 of the Implementing Regulations, a data controller is required to notify the competent authority within 72 hours of becoming aware of a personal data breach, and must also notify impacted individuals without undue delay, if the data breach may cause harm to the individual's data or conflict with their rights or interests;
4. under Article 22 of the PDPL and Article 25 of the Implementing Regulations, data controllers must conduct a data protection impact assessment on data processing that may be considered high risk, such as processing sensitive personal data, combining personal data from different sources, processing using new technologies, automated decision-making and continuous monitoring of individuals; and
5. under Article 29, and as further detailed in the Implementing Regulations on Personal Data Transfers, there are restrictions on transferring personal data outside Saudi Arabia. In order to transfer personal data outside Saudi Arabia, a number of conditions must be met, including that the transfer does not impact national security, that the transfer is limited to the minimum amount of personal data and that there is a specified purpose for the transfer. Certain recipient jurisdictions will be considered 'adequate' on the basis of their level of personal data protection by the competent authority, but transfers to other non-adequate jurisdictions will require further compliance measures, such as putting in place standard contractual clauses with the recipient entity and conducting a transfer impact assessment.

A recent example of such cross-border data transfer arrangements is the framework agreed between Qatar and Saudi Arabia.[107] In September 2024, Qatar and Saudi Arabia signed a framework for the exchange of personal data for security purposes, which took legal effect following Qatar's enactment of Decree No. 30 of 2025 on 14 April 2025.[108-] The framework emphasises compliance with each country's data protection laws and establishes procedures for consent, breach notification, data destruction and regulatory cooperation.

Key administrative provisions include:

1. under Article 31, data controllers are required to maintain a record of their processing activities and make these available to the competent authority on request;
2. under Article 30(4)(c), the competent authority may establish a national register of controllers, and under Article 34 of the Implementing Regulations to the PDPL, the competent authority shall issue rules for controller registration in the national register; and
3. under Article 30(2), the Implementing Regulations to the PDPL will identify situations where data controllers must appoint a data protection officer, and Article

32 of the Implementing Regulations specifies that a data protection officer must be appointed in certain cases, such as where the data controller's primary activities are processing operations that require regular and continuous monitoring of individuals on a large scale, or where the core activities consist of processing sensitive personal data.

In 2024, SDAIA issued a comprehensive set of new regulations, guidance, and documents concerning the PDPL. The updated Transfer Regulations[109] introduce the concept of an adequate country list; however, at the time of writing, this list has not been issued by SDAIA. For countries not considered to be 'adequate', the Transfer Regulations permit transfer subject to the use of SCCs; however, the use of SCCs appears to be limited to specific scenario-based exemptions. This has so far created uncertainty around whether SCCs can be used more broadly, as the Transfer Regulations do not explicitly allow for their general use.

The PDPL contains a number of significant and onerous penalties for noncompliance. Key enforcement powers to note include:

1. under 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 riyals, or both;
2. under Article 36, all other matters of noncompliance may result in a warning or a fine of up to 5 million riyals, which may be doubled for repeat offences;
3. under Article 38, a competent court may order the confiscation of funds obtained as a result of a violation; and
4. individuals can make compensation claims for material or moral damage under Article 40.

Prior to the PDPL, the primary source of data protection law were sharia principles (i.e., Islamic principles derived from the Holy Quran and the Sunna), a number of rights that protect privacy in the Basic Law of Governance 1992 (Royal Order No. A/91 of 1992) (the Basic Law)[110] and sectorial legislation. The PDPL also follows the issuance of National Governance Interim Regulations (the Interim Regulations) published by the NDMO on 1 June 2020.[111] The Interim Regulations contained interim regulations on personal data protection, which applies to all entities in Saudi Arabia that process personal data, as well as entities outside Saudi Arabia that process personal data pertaining to individuals residing in Saudi Arabia, by any means.

The above existing primary sources are still applicable in Saudi Arabia.

For example, Article 40 of the Basic Law mentions privacy as a right that is related to the dignity of an individual and guarantees the privacy of telegraphic and postal communications, and telephone and other means of communication. It also specifies that there shall be no confiscation, delay, surveillance or eavesdropping, except in cases provided by the law.

In addition, there are:

1. sectoral legislation that contains data protection obligations for organisations operating in the financial services, healthcare and telecommunications and IT sectors in Saudi Arabia. For telecommunications and IT in particular, the Telecoms and IT Act imposes data protection obligations on telecommunications or information technology service providers (including digital content platforms), including:
    - a general obligation under Article 23(1) to take measures to protect the confidentiality of a user's information and implement data protection policies;
    - an obligation under Article 23(2) to immediately notify the CST of a data breach; and
    - a requirement under Article 23(3) to retain user information for a period specified by the CST.
2. the CST published 'procedures for launching services or products based on customers' personal data, or sharing personal data',[112] which contain a requirement to conduct a privacy impact assessment and submit this to the CST for acceptance, and 'general principles for personal data protection', which covers data processing principles, obligations on the service provider such as the requirement to implement a privacy programme and customers' rights regarding their personal data;[113]
3. related legislation that contains data protection obligations, for example, the Cloud Computing Services Provisioning Regulations, the Internet of Things Regulatory Framework and the Cyber Law. Article 3 of the Cyber Law states that anyone who spies on, intercepts or receives data transmitted through an information network or a computer without legitimate authorisation or invades an individual's privacy through the misuse of camera-equipped mobile phones, etc., shall be subject to imprisonment for a period not exceeding one year or a fine not exceeding 500,000 riyals, or both;[114] and
4. the extraterritorial scope of foreign data protection legislation that may apply to Saudi companies and individuals by virtue of their overseas activities (e.g., the General Data Protection Regulation (EU) 2016/679 and the United Arab Emirates Federal Decree Law No. 45/2021 on the Protection of Personal Data).

Regarding the processing of children's data, on 25 November 2020, the NDMO published a Children's and Incompetents Privacy Protection Policy,[115] which applies to all entities in Saudi Arabia that collect and process children's personal data, and entities outside of Saudi Arabia that collect the personal data of children residing in Saudi Arabia online. The policy sets out the legal basis for processing children's data and aims to protect children from the negative effects of the internet. The PDPL contains a number of provisions relating to individuals who lack capacity (which would include children) and legal guardians acting on their behalf. Under the PDPL, where consent is the legal basis for processing, consent from a legal guardian is required where the data subject fully or partially lacks legal capacity,[116] and legal guardians can exercise data subject rights on behalf of the data subject who lacks capacity.[117] Personal data cannot be disclosed to third parties where the disclosure conflicts with the interests of a person that fully or partially lacks capacity.[118]

In addition to the discussion above about how cybersecurity concerns are being addressed, the Cyber Law aims to ensure information security, the protection of rights pertaining to the legitimate use of computers and information networks and the protection of public interest, morals and the national economy.

Freedom of expression

Article 8 of the Publications Law also guarantees freedom of expression in different forms of publication.[119]

Although the Basic Law and the Publications Law grant rights promoting self-expression, they are subject to other limits and qualifications laid down by applicable law that aim to protect national interests. Examples of those limits include (without limitation):

1. Article 62 of the Basic Law, which states that if there is an imminent danger threatening the safety of Saudi Arabia, the integrity of its territories or the security and interests of its people, or is impeding the functions of official organisations, the King may take urgent measures to deal with such a danger;
2. Article 6 of the Cyber Law, which criminalises the production, preparation, transmission, or storage of material impinging on public order, religious values, public morals and privacy, through the information network or computers. The penalty for committing any of the foregoing crimes is imprisonment for a term not exceeding five years, and a fine not exceeding 3 million riyals;
3. an Antiterrorism Law introduced in November 2017, which maintains broad definitions of what can be considered a terrorist act. The foregoing law does not restrict the definition of terrorism to violent acts. Other conduct it defines as terrorism includes 'disturbing public order', 'destabilising national security or state stability', 'endangering national unity' and 'suspending the basic laws of governance', all of which may encompass any form of expression; and[120]
4. Article 7(1) of the Tourism Law,[121] which states that disparaging remarks about Saudi Arabia's tourism reputation or touristic sites in Saudi Arabia, as well as any act that results in the devaluation or demotion of these touristic sites, are prohibited by law.

Telecommunications towers

Pursuant to the Telecoms and IT Act, a licence must be obtained from the CST for providing telecommunications services to the public or using a communications network for that purpose, providing infrastructure service for public telecommunications networks, using any numbering resource or frequency spectrum or providing Saudi domain name registration services or establishing centres for registration thereof.[122]

The CST issues two types of licences: individual licences and class licences.[123] Certain services and networks, unless the CST issues an exemption, require an individual licence, such as public mobile cellular telecommunications services and the operation of a public telecommunications network. Service providers in the same class may apply for a Class B licence to provide telecommunications services or operate telecommunication networks

other than the services governed by individual licences.[124] All Class B licences are subject to certain general terms and conditions, and each type of Class B licence is subject to its own special terms and conditions.

Pursuant to the CST Investors' Guide,[125] operators of telecommunications towers must obtain the CST wholesale infrastructure services licence prior to commencing their operations. This licence permits the licensee to own, operate and commercialise telecommunications infrastructure such as towers, small cells, wireless access networks and dark and active fibre. Upon obtaining a licence, the licensee is permitted to provide services and infrastructure to other facilities-based providers and wholesale infrastructure providers licensed by the CST. The CST has complete discretion over which infrastructure elements are included or excluded from the scope of the wholesale licence.

Furthermore, the CST issued the Mobile Towers and Network Sharing Rules[126] (the Colocation Rules), which govern the practice of locating equipment of multiple mobile service providers on a single telecoms tower. The Colocation Rules provide provisions regarding colocation on existing sites, exceptions from the Colocation Rules, passive infrastructure development and upgrades, data sharing and centralisation of information, and pricing provisions for colocation agreements. The Colocation Rules also provide, with respect to commercial colocation agreements, that these commercial agreements shall be based on good faith negotiations. Where a commercial agreement is not reached, related CST regulations or any pricing mechanism decided by CST shall take effect.

The CST also issued the Technical Standards for Outside Plant (OSP) Installations,[127] which contains a number of guidelines concerning the technical requirements of mobile telecommunications towers to be developed. The Standards do not apply to mobile telecommunications towers that already exist. Pursuant to the Standards, mobile telecommunications towers must be designed to accommodate at least three mobile service providers or at least satisfy the business needs of the licensee. The design of all buildings and related structures must use materials, colours, textures, screening and landscaping that will blend the tower facilities to the natural setting and building environment.

E-Delivery platforms

Both the CST and the Transport General Authority (TGA) currently have jurisdiction over commercial activity that connects a business to the end user through an electronic platform. The CST is responsible for regulating the telecommunications aspect of the transaction while the TGA is responsible for regulating the movement of goods that may occur during such activity. However, pursuant to a recent resolution of the Council of Ministers dated 26 July 2022, regulatory oversight for e-delivery platforms has now been ordered to be transferred from the CST to the Ministry of Transport and Logistics Services. August 2023 marked the introduction of the General Plan for Logistics Centers, which aims to develop the infrastructure of Saudi Arabia's logistics sector, diversify the local economy, and strengthen the Kingdom's position as a premier investment destination and a global logistics hub. These logistic centres will enable local industries to efficiently export Saudi products and support e-commerce by facilitating connections between logistics centres and distribution centres within Saudi Arabia’s regions, cities and provinces. Additionally, they will provide high-level tracking capabilities and facilitate the issuance of logistics activity licences, especially after the launch of the unified logistics licence in 2021. Over

1,500 local, regional and international logistics companies have been granted licences, and the 'Fasah' initiative was launched to expedite customs clearance within two hours in cooperation with relevant government entities.[128]

The CST issued the Regulations for Delivery Service Provision via E-Platform[129] (the Delivery Service Regulations), which provides that any service provider must register with the CST as such. 'Service provider' is defined as any person who connects a delivery agent with a consumer through an electronic platform. The Delivery Service Regulations also include a number of operational measures that service providers must adhere to, including the creation of a call centre to receive customer queries and complaints, a clear display of the services provided and the prices for each service, and providing electronic receipts, or text messages containing the details of the order and the price, for each financial transaction, among others.

Furthermore, the TGA issued the Regulations for E-Hailing Freight Transport Vehicles[130-] (the E-Hailing Regulations) amended in December 2023, which aim to improve service quality and attract investment into the industry by streamlining operational procedures and outlining the fines and penalties for noncompliance. The E-Hailing Regulations target private and family fare-service providers, ride-hailing companies and public transportation operators.

Space and satellites

Satellites and other space technologies are expected to play an increasingly important role in Saudi Arabia's digital infrastructure and economy.

In 2022, the Supreme Space Council was established to oversee the strategy of development of the space sector. During the same year, CITC was renamed CST, recognising the importance of integration of communications, space and technology.[131]

In 2023, the CST published for consultation 'Space Data Regulations Platform and Application Document for Obtaining a Permit to Provide a Space Data Platform Services', aiming to establish a regulatory environment of the space sector and make space data governance more effective. The draft includes guideline and requirements for entities interested in acquiring the space sector licence, as well as obligations of relevant parties to ensure user rights and data security.[132]

In 2025, the CST released the Non-Terrestrial Networks (NTN) regulations, comprising three documents focused on operation services, telecommunication services and space station registration. These regulations aim to foster a supportive regulatory environment to attract investment, facilitate the adoption of advanced NTN wireless technologies, and enhance the digital economy in Saudi Arabia by enabling technologies such as Air-to-ground communication, Mega Constellations, and Satellite IoT.[133]

CST issued the Earth Observation (EO) Platform Regulations and a document titled 'Application for Obtaining a Permit to Provide Earth Observation (EO) Platform Service' with the aim of creating an appropriate environment to enable the private sector to establish and develop the earth observation services market and emerging businesses therein, and to stimulate its contribution to raising the Kingdom's gross domestic product through the development of value-added products.

Spectrum policy

Development

The following pieces of legislation regulate this area.

The Telecom Act

The regulation of radio spectrum usage is one of the main functions of the CST pursuant to the Telecom Act. Under the Telecom Act, an essential objective of spectrum management is to promote optimal spectrum use by achieving optimum utilisation of this resource, ensuring the creation of a favourable atmosphere to promote and encourage fair competition in all fields of telecommunications, ensuring effective and interference-free usage of frequencies, ensuring clarity and transparency of procedures, ensuring principles of equality and non-discrimination, and ensuring the development of telecommunications technology.

The Telecoms and IT Act

Pursuant to the Telecoms and IT Act, radio spectrum usage remains under the jurisdiction of the CST. The CST is also empowered under the Telecoms and IT Act to collect the specified amounts for the licensing of spectrum usage and penalise offenders accordingly. The Telecoms and IT Act also introduces restrictions prohibiting services providers who control a certain market from denying access to other service providers, with the threshold of control being 40 per cent of the relevant market, subject to the CST's judgement based on market conditions.

The National Spectrum Strategy 2025

The CST has published a National Spectrum Strategy 2025[134] in 2020, which describes the CST's priorities with respect to the development of Saudi Arabia's spectrum policy going forward. The Spectrum Strategy states that Saudi Arabia achieved considerable success in assigning spectrum to public mobile networks that utilise international mobile telecommunications standards to provide mobile broadband services and notes the creation of a dedicated subcommittee in 2019 under the auspices of the CST to focus on 5G spectrum matters within the National 5G Taskforce.

In June 2025, the CST published its Spectrum Outlook for Commercial and Innovative Use (2025–2027), aiming to optimise radio spectrum use to drive digital transformation, economic growth and global competitiveness in Saudi Arabia. The plan supports multiple sectors by enabling advanced solutions, expanding telecommunications coverage and promoting efficient spectrum use through modern regulatory frameworks, including support for NTN and Fixed Wireless Access. By fostering innovation and partnerships, particularly in 6G networks, the outlook seeks to position the Kingdom as a global digital investment hub, with stakeholder feedback from various sectors shaping its development.[135]

Flexible spectrum use

Under the Spectrum Strategy, a comprehensive review of fixed point-to-point links is contemplated to determine the most optimal band plans with the overall objective being to review and optimise a total of 5.4GHz of legacy spectrum by 2025.

Currently, the Spectrum Strategy notes that Saudi Arabia has made notable progress on addressing issues related to the international mobile telecommunications (IMT) field, which resulted in the country's ranking among the leading nations in awarded IMT spectrum. In March 2021, the CST issued a plan for the allocation and use of spectrum bands identified for IMT (the IMT Spectrum Plan),[136] aimed at identifying the frequency allocation and use regulations for radio spectrum bands identified for IMT services. Furthermore, the Spectrum Strategy also speaks of enabling space spectrum in which the focus would be on championing Saudi Arabia's emerging space industry in international discussions and within Saudi Arabia. This will enable the CST to work on satellite coordination requests and resolve these requests in a timely manner, thereby allowing existing and future satellite services access to spectrum and manage trade-offs with IMT allocations.

Broadband and next-generation services spectrum use

The Spectrum Strategy recognises a number of ways in which the growing need for spectrum for broadband services and next-generation services, among other things, is addressed. The Spectrum Strategy states that it aims to identify and resolve existing inefficiencies while overcoming hurdles that prevent international harmonisation and optimal spectrum utilisation. Moreover, there is a push for 5G+ deployment to position Saudi Arabia among the leading nations in unlocking innovative high-performance use cases and applications based on 5G.

Spectrum auctions and fees

Auctioning spectrum

As of the third quarter of 2023, the CST auctioned spectrum to licensed mobile networks operators within Saudi Arabia.

In 2017, the CST issued a press release stating that it had awarded large blocks of contiguous spectrum, ideal for deployment of next-generation broadband networks across Saudi Arabia to four mobile network operators (MNOs).[137] This was the first spectrum auction in Saudi Arabia and the first time that a spectrum in the 700MHz band was allocated in the MENA region.

The auction raised 5.8 billion riyals for 50MHz in the 700MHz band and 66MHz in the 1,800MHz band.

We are not aware of any plans to auction spectrum to non-licensed entities.

Additionally, the CST published a public consultation on 30 May of 2021 on an upcoming spectrum auction during which it aims to release multiple bands for a wide range of digital

radio services. The CST's released statement noted that the CST is inviting all national and international parties to provide their feedback and engage in this process no later than 26 July 2021. The public consultation announcement noted that CST has started preparations for a spectrum auction during the second half of 2021 that will include spectrum in the following bands: 600MHz FDD, 700MHz FDD, 700MHz SDL, 1980–2010/2170–2200MHz FDD and 3800–4000MHz TDD, in addition to 2×5MHz each in the 410–430MHz and 450–480MHz bands either as part of the auction or separately.

CST then published a public consultation on 7 October 2021 on an upcoming spectrum auction of 2100MHz for non-terrestrial networks. CST intends to hold this auction by the end of 2021, for the 2100MHz (30×2MHz) band, as part of the implementation process for 'Spectrum Outlook for Commercial and Innovative Use 2021–2023' in Saudi Arabia. The CST's released statement noted that the CST is inviting all national and international parties to provide their feedback and engage in this process no later than 30 October 2021. Based on the responses received by CST on its public consultation issued on 30 May 2021 (referenced above), the CST updated the timeline of the spectrum auctions to have two auctions for 2100MHz in the fourth quarter of 2021, and for 600, 700, 700 SDL and 3800MHz in the first quarter of 2022. On 27 February 2022, the CST published a public consultation on the information memorandum and auction rules for the fifth spectrum auction for IMT systems for the award of 600, 700 and 3800 MHz spectrum bands through auction set on 19 June 2022. In December 2022, the auction was awarded to one of the publicly listed telecommunications provider.

Spectrum auctions are open to both entities that hold a Facilities-Based Unified Telecommunications Services License (USL) as well as entities that can demonstrate that they are already providing services in the S-Band. Any successful bidder that already holds a USL can provide any terrestrial or non-terrestrial service using the spectrum acquired in the auction. However, applicants that do not already hold a USL will need to apply for a separate Class B licence to provide any specific telecommunications service at application.

CST published the information memorandum and rules for this auction, which aims to allow licensed service providers to participate.[138] The auction seeks to improve 5G coverage in remote areas, enhance service quality on roads, border entries and railways, increase internet speeds for customers and promote investment and competition in wireless services. CST clarified that this auction will further solidify the Kingdom's leadership role in the ICT sector. It is part of the 'Spectrum Outlook for Commercial and Innovative Use 2021–2023,' published in 2020, and aligns with CST's strategic goals for enabling 5G networks in the Kingdom. Saudi Arabia will become the first country in the Middle East, Europe, and Africa to assign the 600 MHz band for IMT and will have the highest assigned IMT spectrum globally in bands below 5GHz. The information memorandum includes auction design elements and rules, such as allocating channel blocks for different domains, technical and regulatory conditions, eligibility criteria, opening prices and obligations for the channel blocks.

In its most recent spectrum auction, announced on 11 November 2024, CST awarded spectrum in the 600, 700 and 3800MHz frequency bands to STC, Mobily and Zain. The auction is expected to contribute over 25 billion riyals to Saudi Arabia's GDP by 2030 by enhancing digital infrastructure, promoting investment and supporting the deployment of advanced telecom services.[139]

Spectrum trading

The CST issued its Spectrum Trading Regulations in August 2022.[140] The Spectrum Trading Regulations are intended to enhance flexibility in respect of access to spectrum usage by adopting new methods for the reallocation of frequencies between users, and to enable trading of spectrum usage rights in secondary markets. The trading of spectrum usage rights under the Spectrum Trading Regulations may be partial or full and must be notified to CST for its approval or non-objection thereof. The Spectrum Trading Regulations further specify information and provisions to be covered by any spectrum trading agreement.

Spectrum fees

Currently, spectrum users must be licensed by CST and the licence is accompanied by a fee to be paid to the CST calculated in accordance with CST's Frequency Licensing Fees Regulations.[141]

Media

Regulation of media distribution generally

In addition to the key laws regulating media and media protection specified under 'Main sources of law', the following laws are also relevant in regulating media and media protection in Saudi Arabia:

1. the Media Policy in Saudi Arabia issued by the MoM;[142]
2. the GCAM age classification guide;
3. the Telecoms and IT Act; and
4. the Digital Platform Regulations.

As above, the draft Media Law, once – or if – it comes into effect, will replace the GMAR Regulations and the Publications Law. As this has not come into effect at the time of writing, the below focuses on existing laws as well as updates under the draft Media Law.

The media sector may be broadly categorised into the following subsectors: publications, press institutions and audiovisuals. This chapter predominantly focuses on audiovisuals.

As noted above, in September 2023, GAMR replaced GCAM, and has a wider supervisory jurisdiction covering all forms of media. Under the GAMR Regulations, GAMR may propose draft laws and regulations relevant to the media sector. For example, GAMR is implementing media regulation guidelines aimed at clarifying content violations to assist content creators in compliance and prevent infractions.[143]

Service obligations

In order to engage in broadcasting and other audiovisual media activity in Saudi Arabia, an appropriate licence needs to be obtained. The types of licences contemplated by the Audiovisual Media Law include:

1. media content production, and operating media production studios;
2. advertising agencies;
3. operating cinemas;
4. satellite distribution;
5. terrestrial transmission;
6. satellite uplink stations;
7. linear and non-linear (e.g., video-on-demand and over-the-top) broadcasting;
8. radio broadcasting;
9. IPTV and cable television;
10. media audience measurement; and
11. importation, distribution, sale and lease of:
    - audiovisual media content;
    - cinematic movies, videos and TV shows; and
    - receivers and accessories.

Licensees are required to pay the applicable fees and comply with the requirements specified in the licence. Furthermore, licensees are required to (among other things): (1) comply with the GAMR's policies with regard to prioritising the use of Saudi Arabia's resources, including human resources; and (2) participate in capacity building in respect of local content production capabilities.

Licensees may need to comply with technical specifications for equipment used in the transmission and reception of media content, and with the allocation of frequencies and associated technical procedures and standards for frequency use.

Under Article 3 of the draft Media Law, the Regulations shall determine the types of licences required for all traditional and electronic media activities (such as newspapers, electronic publishing, media broadcasting, media production, radio and TV artistic production, cinemas, electronic games and adverts), so there may be updates to the current licensing requirements. Article 10 of the draft Media Law contains a list of obligations on licensees, which includes maintaining a full list of the materials broadcast for 90 days, lodging copied of printed media, prioritising the use of Saudi Arabia resources and developing national production and broadcasting capabilities (as above). Penalties for violations of the draft Media Law include fines of up to 10 million riyals (which may be doubled in cases of repetition), temporary suspensions of activities for up to six months, closing or blocking the place of violation (either temporarily or permanently), suspension or removal of the licence and the requirement to publish an apology.

The CST's Digital Platform Regulations includes licences and registration requirements for various content platforms. In addition to licences and registration requirements, service

providers are required to comply with relevant regulations from competent authorities including those concerning content, user protection and data protection, to appoint a platform compliance officer and to cooperate with the CST's requests for information.

Further, GAMR is also now determining fees for issuing licences for media activities and setting the relevant controls and procedures for licencees.

Content restrictions

Article 9 of the draft Media Law lists media content that may not be published, which includes any media that:

1. prejudices the principles of Islamic sharia or the supreme interests of Saudi Arabia;
2. threatens national or international peace;
3. instigates the committing of crime or violence, breaches national security, public order, public morals or public health;
4. infringes the rights of others;
5. instigates racism, national or religious hatred; or
6. promotes drugs, alcohol or tobacco.

Article 13 requires that media content be submitted to GAMR for approval before circulation.

The Copyright Law protects original and derivative works created in the fields of literature, art and sciences, irrespective of their type, means of expression, importance or purpose of authorship.

The Copyright Law is intended to prevent third parties from copying the protected work. The protection period for sound works, audiovisual works, films, collective works and computer programs is 50 years from the date of the first show or publication of the work, regardless of republication. The protection period for broadcasting organisations shall be 20 years from the date of the first transmission of programmes or broadcast materials, and the protection period for the producers of sound recordings and performers shall be 50 years from the date of performance or its first recording, as the case may be.

Cabinet Resolution No. 163 dated 10/24/1417H prohibits users within Saudi Arabia from publishing or accessing illegal, harmful or anti-Islamic content on the internet.

The CST is responsible for administering an internet filtering service, which limits certain content on the internet and restricts access to specific internet services.[144] Under the Telecoms and IT Act it is an offence to bypass the internet filtering, facilitate internet circumvention or to provide any assisting tools for doing so.[145] Violating internet filtering requirements under the Telecoms and IT Act may result in penalties including a fine of up to 25 million riyals, revocation of a licence or blocking of a service.

The authorities achieved significant progress through daily proactive monitoring and cooperation with partners in the Electronic Commerce Council and the Permanent Internet Security Committee. The CST provides these services in collaboration with the Permanent Internet Security Committee and supplies data service providers with a list of banned

websites. Alternatively, users may submit a request to block a particular website where they deem the website or material to contain undesirable content. Once a user submits the web-based form, it is reviewed by a team of CST employees who determine whether the user's request is justified.

The data service providers are responsible for ensuring that the websites are banned on their internet gateways. If a data service provider fails to comply with the CST's instructions, it may result in a fine of up to 5 million riyals.[146]

In terms of the content that is filtered, websites and materials that are inconsistent with Islam – for example, materials relating to pornography, gambling and drugs – would be classified as harmful content.

The CST regulates network operators, the ICT and the postal sector. The Telecoms and IT Act provides the legal framework for organising this last sector.[147]

As noted above, in September 2023, GAMR replaced GCAM, and has a wider supervisory jurisdiction covering all forms of media, and the MoM supervises all means of visual, audio and written communication content in Saudi Arabia.[148]

Pursuant to the Publications Law, a licence from the MoM is required to carry out, among other things, the following activities:

1. printing, publishing or distributing publications or engaging in any other publication services;
2. importing, selling or renting movies or video tapes;
3. producing, selling or renting computer programs;
4. engaging in any press services; and
5. carrying out photography services.

The activities mentioned above may only be carried out by Saudi nationals. In addition, the holder of a licence may transfer, lease or share ownership of such licence after obtaining the MoM's approval.

The author, publisher, printer or distributor must obtain the MoM's approval prior to circulating such publication. The MoM will not approve a publication that prejudices Islam, the Saudi Arabia regime, the interests of the country or public morals and customs.

As such, we understand that traditional media outlets would fall under the remit of the Publications Law.

As described more fully above, there are three types of licences that can be obtained from the GAMR: media activity licences; cinema licences; and broadcasting and distribution licences. As such, we understand that emerging platforms are more likely to fall within the GAMR Regulations and GAMR Implementing Regulations. As noted above, in September 2023, GAMR replaced GCAM, and has a wider supervisory jurisdiction covering all forms of media, including in relation to licences; however, at the time of writing there is limited information available on GAMR.

Content restrictions are also imposed under the Cloud Computing Services Provisioning Regulations. Article 3.5.2 of the Cloud Computing Services Provisioning Regulations states

that cloud service providers are not liable for unlawful content or infringing content that was uploaded, processed or stored on the cloud service providers' systems, and Article 3.5.3 of the Cloud Computing Services Provisioning Regulations states that there is no legal obligation on cloud service providers to monitor their systems for unlawful or infringing content. However, Article 3.5.4 of the Cloud Computing Services Provisioning Regulations states that cloud service providers must remove unlawful or infringing content or render it inaccessible within the country after written notice by the CST or any other authorised entity, or per Article 3.5.5, may do so on its own initiative or following a third-party request.[149]

In addition, mandatory controls are required for posting adverts on social media platforms, including clearly announcing that the content is an advert,[150] not including false or misguiding information, and not posting adverts for counterfeit or fraudulent products.[151]

Under the CST's Digital Platform Regulations, service providers are required to comply with local content restrictions.

GAMR and the CST confirm their commitment to regulating content standards by publishing details of some of their activities, including requesting digital content providers to remove certain content and adverts that do not comply with content standards and fining social media users who publish offending content.

A recent example is the enforcement action taken by GAMR in September 2025 against the online gaming platform Roblox, which required the temporary suspension of text and voice chat, the blocking of over 300,000 non-compliant 'social gathering' games, and enhancements to Arabic-language moderation through the hiring of local moderators and upgraded content filters. These measures were aimed at protecting minors from harmful interactions and ensuring that Roblox's operations align with Saudi cultural and regulatory standards. This development underscores GAMR's increasing oversight of global digital platforms and its ongoing commitment to safeguarding users within the Kingdom.[152]

Internet-delivered video content

There is limited information on how the move from broadcast video distribution to internet video distribution affected consumers and the ability of internet service providers to control, and be compensated for, the content being transmitted over their networks.

However, according to the MCIT's 2022 Annual Report, the MCIT committed to provide high-quality communications and internet services with a coverage rate of 100 per cent even in remote areas of Saudi Arabia.[153] Currently, 98 per cent of Saudi regions have 4G coverage,[154] and 98.6 per cent of the population are internet users.[155]

In addition, Saudi Arabia has a 'KSA Free Wifi Initiative',[156] which gives users access to free connectivity in 60,000 Wi-Fi hotspots in public places across Saudi Arabia.

The Digital Content Council also announced a programme called Ignite, which aims to transform Saudi Arabia into a digital content hub and triple Saudi Arabia's digital content market size in gaming, audio, video and advertising.[157]

'Ignite the Ads', a digital advertising event organised by the Digital Content Council and the MCIT in Saudi Arabia took place at Riyadh's King Abdullah Financial District Conference Center from 28 to 31 May 2024. The event brought together startups, entrepreneurs and

advertising professionals. The first two days were dedicated to business networking, while the last two focused on brand awareness, social media, and marketing strategies. As part of Saudi Arabia's Ignite program, the event highlighted the programme's 70 per cent year-on-year growth to 20 billion riyals in 2023.

Outlook and conclusions

In the 2025 Global Innovation Index (GII) published by the World Intellectual Property Organisation, Saudi Arabia is ranked 46th among 139 economies, continuing its upward trajectory in global innovation performance. Within the high-income group of 54 economies, Saudi Arabia stands at 40th, and it ranks fifth among 18 economies in Northern Africa and Western Asia. Since 2020, Saudi Arabia has advanced twenty places in the GII, moving from 66th in 2020 and 2021 to 51st in 2022, 48th in 2023 and 46th in 2025.

Notable strengths include a top-tier innovation input profile (31st) and world-class digital indicators, with first place globally for ICT use and fourth for government online services. Saudi Arabia also ranks third worldwide for the state of cluster development and performs strongly in general infrastructure (16th).

The technology, media and telecommunications sectors are core to the future economic development of Saudi Arabia and, accordingly, it is likely that we will see further legislative and regulatory developments with respect to these sectors over the next few years.

It continues to be a very exciting time to be a TMT lawyer operating in Saudi Arabia.

Endnotes

1 https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf. ^ Back to section

2 https://sdaia.gov.sa/Documents/RegulationonPersonalDataEN.pdf. ^ Back to section

3 https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf. ^ Back to section

4 https://sdaia.gov.sa/Documents/CommonRulesBCRForPersonalDataTransferEN.pdf. ^ Back to section

5 https://sdaia.gov.sa/en/SDAIA/about/Documents/RulesforAppointingPersonalDataProtectionOfficer.pdf. ^ Back to section

6 https://sdaia.gov.sa/Documents/PrivacyPolicyGuideline.pdf. ^ Back to section

7 https://sdaia.gov.sa/Documents/MinmumPDGuideline.pdf. ^ Back to section

8 https://sdaia.gov.sa/Documents/PersonalDataDestructionAnonymizationAndEncryptionGuideline.pdf. ^ Back to section

9 https://sdaia.gov.sa/Documents/PersonalDataDisclosureCasesGuideline.pdf. ^ Back to section

10 https://sdaia.gov.sa/Documents/PersonalDataProcessingActivitiesRecordsGuideline.pdf. ^ Back to section

11 https://sdaia.gov.sa/Documents/RegulationonPersonalDataEN.pdf. ^ Back to section

12 https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf. ^ Back to section

13 https://sdaia.gov.sa/Documents/CommonRulesBCRForPersonalDataTransferEN.pdf. ^ Back to section

14 https://sdaia.gov.sa/en/SDAIA/about/Documents/RulesforAppointingPersonalDataProtectionOfficer.pdf. ^ Back to section

15 https://sdaia.gov.sa/ar/SDAIA/eParticipation/Files/Rules-Governing-en.pdf. ^ Back to section

16 https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf. ^ Back to section

17 https://sdaia.gov.sa/en/SDAIA/about/Documents/ExecutiveRegulations.pdf. ^ Back to section

18 https://www.mcit.gov.sa/en. ^ Back to section

19 https://www.cst.gov.sa/en/Pages/default.aspx. ^ Back to section

20 https://nca.gov.sa/en/. ^ Back to section

21 https://cert.gov.sa/en/about-us/. ^ Back to section

22 https://www.media.gov.sa/en. ^ Back to section

23 https://www.gamr.gov.sa. ^ Back to section

24 https://www.mcit.gov.sa/en/news/digital-content-council-allocates-sar-42-billion-support-creators-and-develop-promising. ^ Back to section

25 https://www.gcam.gov.sa. ^ Back to section

26 https://media.gov.sa/en/news/5563. ^ Back to section

27 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/RD.aspx. ^ Back to section

28 https://www.cst.gov.sa/ar/Decisionsoffers/Decisions/Documents/DRP_Guidelines_Final.pdf. ^ Back to section

29 Regulations available to download on https://www.cst.gov.sa/en/Pages/default.aspx. ^ Back to section

30 https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-1605. ^ Back to section

31 https://sdaia.gov.sa/en/SDAIA/about/Pages/organizationalStructure.aspx. ^ Back to section

32 https://sdaia.gov.sa/. ^ Back to section

33 https://ncdc.gov.sa/. ^ Back to section

34 https://saber.sa/. ^ Back to section

35 https://ndu.mcit.gov.sa/en. ^ Back to section

36 https://www.saip.gov.sa/en/. ^ Back to section

37 See https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/ for further information. ^ Back to section

38 https://www.saudiembassy.net/bureau-investigation-and-prosecution. ^ Back to section

39 https://nca.gov.sa/en/pages/ecc.html. ^ Back to section

40 https://nca.gov.sa/ccc-en.pdf. ^ Back to section

41 https://nca.gov.sa/en/regulatory-documents/guidelines-list/1360/. ^ Back to section

42 https://nca.gov.sa/news?item=373. ^ Back to section

43 https://nca.gov.sa/en/news/1458/. ^ Back to section

44 https://cert.gov.sa/en/. ^ Back to section

45 https://nca.gov.sa/ar/news/1/. ^ Back to section

46 https://help.nic.sa/en/rules/. ^ Back to section

47 https://www.arabnews.com/node/2617421/business-economy. ^ Back to section

48 https://nca.gov.sa/ar/news/1/. ^ Back to section

49 https://www.mcit.gov.sa/en/news/digital-content-council-allocates-sar-42-billion-support-creators-and-develop-promising. ^ Back to section

50 https://www.cst.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf. ^ Back to section

51 https://www.cst.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_002_E_CITC%20Ordinance.pdf. ^ Back to section

52 https://mc.gov.sa/en/Regulations/Pages/details.aspx?lawId=aaa4d4cf-ca57-41ff-a3f9-aa8500a3512c&hw=e-commerce. ^ Back to section

53 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/default.aspx. ^ Back to section

54 https://regulations.citc.gov.sa/PublishedDocuments/GovernorApprovalDecision_465/b1d3c2f6-5423-482b-aec7-bfa7287975d7_Regulations%20for%20Cybersecurity%20Operations%20in%20ICT%20%20Postal%20Sector.pdf. ^ Back to section

55 https://regulations.citc.gov.sa/PublishedDocuments/GovernorApprovalDecision_1481/4e66ebac-7547-4a2e-93bb-0110ba6f6450_Regulations%20for%20Providing%20Digital%20Content%20Platform%20Services.pdf. ^ Back to section

56 https://istitlaa.ncc.gov.sa/en/transportation/citc/crdcp/Pages/default.aspx. ^ Back to section

57 https://istitlaa.ncc.gov.sa/en/transportation/citc/dcr/Documents/Data%20Center%20Regulation.pdf. ^ Back to section

58 https://istitlaa.ncc.gov.sa/ar/transportation/citc/crdcp/Pages/default.aspx. ^ Back to section

59 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf. ^ Back to section

60 https://regulations.citc.gov.sa/PublishedDocuments/GovernorApprovalDecision_1483/58fd86fe-c778-49c4-9b25-d0f0370db70b_Regulations%20for%20Providing%20Electronic%20Aggregation%20in%20Telecommunications%20Services.pdf. ^ Back to section

61 https://www.cst.gov.sa/ar/RulesandSystems/RegulatoryDocuments/ReductionofSPAM/Documents/IT%20008%20E%20-%20Regulation_For_The_Reduction_of_SPAM_Eng.pdf. ^ Back to section

62 https://regulations.citc.gov.sa/PublishedDocuments/GovernorApprovalDecision_1532/d4ec4caa-8b28-46d1-bdbd-81268b573025_%D8%AA%D9%86%D8%B8%D9%8A%D9%85%D8%A7%D8%AA%20%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA%20%D8%A7%D9%84%D8%A3%D8%B4%D9%8A%D8%A7%D8%A1%20.pdf and https://www.cst.gov.sa/en/media-center/news/CST-Updated-the-IoT-Regulatory-Framework-Document-and-Cha ^ Back to section

63 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Licenses/LicensingRegulatoryFrameworks/Documents/PL-SP-021-A-MVNO-EN.pdf. ^ Back to section

64 https://help.nic.sa/en/regulation/. ^ Back to section

65 https://help.nic.sa/en/rules/. ^ Back to section

66 https://www.nic.sa/en/. ^ Back to section

67 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/ICTInfrastructure.aspx. ^ Back to section

68 https://mutasil.cst.gov.sa/#/publicDecisionDetails/1536. ^ Back to section

69 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/default.aspx. ^ Back to section

70 https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/2. ^ Back to section

71 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCSPR_EN.pdf. ^ Back to section

72 https://nca.gov.sa/en/pages/ecc.html. ^ Back to section

73 https://nca.gov.sa/ar/ccc-en.pdf. ^ Back to section

74 https://istitlaa.ncc.gov.sa/en/Security/nca/ECC22024/Pages/default.aspx. ^ Back to section

75 https://nca.gov.sa/ar/news/1558/ and https://cdn.nca.gov.sa/api/files/public/upload/86e09090-44e4-481f-bc28-355673607654_ECC--2024-EN.pdf. ^ Back to section

76 https://www.spa.gov.sa/en/N2062495. ^ Back to section

77 https://regulations.citc.gov.sa/PublishedDocuments/GovernorApprovalDecision_465/b1d3c2f6-5423-482b-aec7-bfa7287975d7_Regulations%20for%20Cybersecurity%20Operations%20in%20ICT%20%20Postal%20Sector.pdf. ^ Back to section

78 https://investmentpolicy.unctad.org/investment-policy-monitor/measures/4287/saudi-arabia-launches-four-special-economic-zones-sez-#:~:text=The%20new%20SEZs%20are%20spread,5%25%20Corporate%20Income%20Tax%20rate-. ^ Back to section

79 https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Cyber%20Security%20Framework.pdf. ^ Back to section

80 https://cma.org.sa/en/RulesRegulations/Guides/Documents/Cyber_Security_en.pdf. ^ Back to section

81 https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf. ^ Back to section

82 https://sdaia.gov.sa/en/SDAIA/about/Documents/ExecutiveRegulations.pdf. ^ Back to section

83 https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf. ^ Back to section

84 https://sdaia.gov.sa/Documents/CommonRulesBCRForPersonalDataTransferEN.pdf. ^ Back to section

85 https://istitlaa.ncc.gov.sa/en/Transportation/NDMO/IRofPDPLAmendments/Pages/default.aspx. ^ Back to section

86 https://dgp.sdaia.gov.sa/wps/portal/pdp/services/details/Regulatorysandboxprogram/!ut/p/z1/jY_BDsFAFEW_x ^ Back to section

87 https://alwatannews.net/international/article/4058203/. ^ Back to section

88 https://istitlaa.ncc.gov.sa/en/media/sbauthority/signalsba/Pages/default.aspx# ^ Back to section

89 https://gcam-website.s3.amazonaws.com/Gamr_Assets/%D8%A7%D9%84%D9%84%D8%A7%D9%8A%D9%94%D8%AD%D8%A9.pdf. ^ Back to section

90 https://regulations.citc.gov.sa/PublishedDocuments/GovernorApprovalDecision_1481/4e66ebac-7547-4a2e-93bb-0110ba6f6450_Regulations%20for%20Providing%20Digital%20Content%20Platform%20Services.pdf. ^ Back to section

91 https://www.cst.gov.sa/en/mediacenter/pressreleases/Pages/2023110201.aspx. ^ Back to section

92 https://istitlaa.ncc.gov.sa/en/Transportation/citc/GlobalDigital/Pages/default.aspx. ^ Back to section

93 https://www.cst.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf. ^ Back to section

94 https://www.cst.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_002_E_CITC%20Ordinance.pdf. ^ Back to section

95 https://nca.gov.sa/en/registration-and-licensing/. ^ Back to section

96 https://dgp.sdaia.gov.sa/wps/wcm/connect/ae62a272-e9ab-46dd-9666-33e818bfd049/The+Rules+Governing+the+National+Register+of+Controllers+Within+the+Kingdom-public.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE-ae62a272-e9ab-46dd-9666-33e818bfd049-p2s25P-. ^ Back to section

97 https://www.sharikatmubasher.com/news/article/21508573/misa-unveils-national-program-to-boost-entrepreneu ^ Back to section

98 https://gac.gov.sa/index_en.asp. ^ Back to section

99 https://www.linkedin.com/posts/talal-alhogail-m-a-000a6a116_merger-review-guidelines-ugcPost-6848551624420450304-B0QD. ^ Back to section

100 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/ProceduralRulesForMergersAndAcquisitions.pdf. ^ Back to section

101 https://hrsd.gov.sa. ^ Back to section

102 https://www.cst.gov.sa/en/USF/Pages/About.aspx. ^ Back to section

103 Article 1 of the Universal Access and Universal Service Policy. ^ Back to section

104 https://www.cst.gov.sa/en/USF/Pages/Projects.aspx. ^ Back to section

105 https://www.cst.gov.sa/ar/RulesandSystems/RegulatoryDocuments/Documents/Termstelecomservices_en.pdf. ^ Back to section

106 Article 2(1), PDPL. ^ Back to section

107 https://www.spa.gov.sa/en/N2255660. ^ Back to section

108 https://almeezan.qa/LawView.aspx?LawID=10006&language=ar&opt. ^ Back to section

109 https://sdaia.gov.sa/Documents/RegulationonPersonalDataEN.pdf. ^ Back to section

110 https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/16b97fcb-4833-4f66-8531-a9a700f161b6/1. ^ Back to section

111 https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf. ^ Back to section

112 https://www.cst.gov.sa/en/RulesandSystems/privacy/Documents/Procedures-data-privacy-en.pdf. ^ Back to section

113 https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-404. ^ Back to section

114 https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/2. ^ Back to section

115 https://sdaia.gov.sa/ndmo/Files/Policies002.pdf. ^ Back to section

116 Article 5(1), PDPL. ^ Back to section

117 Article 3(3), PDPL Implementing Regulations. ^ Back to section

118 Article 16(6), PDPL. ^ Back to section

119 https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/ecaaec43-8ff9-46b8-b269-a9a700f16e66/2. ^ Back to section

120 'Terrorist crime' means any act committed, individually or collectively, directly or indirectly, by a perpetrator, with the intention to disturb public order, destabilise national security or state stability, endanger national unity, suspend the Basic Law or some of its articles, undermine state reputation or status, cause damage to state facilities or natural resources, attempt to coerce any of its authorities into a particular action or inaction or threaten to carry out acts that would lead to the aforementioned objectives or instigate such acts; or any act intended to cause death or serious bodily injury to a civilian, or any other person, when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act. ^ Back to section

121 https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/7d777c66-d28b-43de-9305-af23013b1738/1. ^ Back to section

122 https://www.cst.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf. ^ Back to section

123 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Licenses/BylawProvisionsForTelecommunicationsLicenses/Pages/Article11.aspx. ^ Back to section

124 https://www.cst.gov.sa/en/services/licensing/Pages/LicensingRequirementsTypeB.aspx. ^ Back to section

125 https://www.cst.gov.sa/ar/services/licensing/documents/investorguideen.pdf. ^ Back to section

126 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/RD.aspx. ^ Back to section

127 https://www.cst.gov.sa/ar/Decisionsoffers/Decisions/Documents/attach392_2.pdf. ^ Back to section

128 https://mot.gov.sa/en/AboutUs/Pages/Brief.aspx. ^ Back to section

129 https://www.cst.gov.sa/en/services/licensing/Documents/Decisions-en-app.pdf. ^ Back to section

130 https://tga.gov.sa/Regulations/Read/4. ^ Back to section

131 https://www.cst.gov.sa/en/AboutUs/Pages/History.aspx. ^ Back to section

132 https://www.cst.gov.sa/en/mediacenter/pressreleases/Pages/2023082701.aspx. ^ Back to section

133 https://www.cst.gov.sa/en/about/program-and-initiatives/Non-Terrestrial-Networks-Program. ^ Back to section

134 https://www.cst.gov.sa/ar/services/spectrum/Documents/National%20Spectrum%20Strategy_E.pdf. ^ Back to section

135 https://www.cst.gov.sa/en/media-center/news/N2025063001. ^ Back to section

136 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/FrequencySpectrum/Documents/SM-Regulation%20and%20Allocation%20for%20Spectrum%-20Bands%20Identified%20for%20IMT.pdf. ^ Back to section

137 https://www.cst.gov.sa/en/MediaCenter/PressReleases/Pages/2017060601.aspx. ^ Back to section

138 https://www.cst.gov.sa/en/mediacenter/pressreleases/Pages/202291601.aspx. ^ Back to section

139 https://www.cst.gov.sa/en/business/media-center/news/CST-Announces-the-Winners-of-the-Spectrum-Auction- ^ Back to section

140 https://regulations.cst.gov.sa/#/publicDecisionDetails/467. ^ Back to section

141 https://www.cst.gov.sa/en/RulesandSystems/Bylaws/Pages/FinancialSpectrumPolicy.aspx. ^ Back to section

142 An official English translation is unavailable on the MoM's website. ^ Back to section

143 https://saudigazette.com.sa/article/655387. ^ Back to section

144 Article 24(1), PDPL. ^ Back to section

145 Article 24(2), PDPL. ^ Back to section

146 Freedom of the Net 2019, Saudi Arabia, Freedom House. ^ Back to section

147 https://www.cst.gov.sa/en/AboutUs/AreasOfwork/Pages/default.aspx. ^ Back to section

148 https://www.my.gov.sa/wps/portal/snp/pages/agencies/agencyDetails/AC164/. ^ Back to section

149 https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf. ^ Back to section

150 Article 10 of the Implementing Regulations of the E-Commerce Law. ^ Back to section

151 Article 12 of the E-Commerce Law. ^ Back to section

152 https://saudigazette.com.sa/article/654724. ^ Back to section

153 Page 12 of the MCIT's 2022 Annual Report: https://www.mcit.gov.sa/sites/default/files/2023-07/MCIT_Annual%20Report_2022_En-Web_0.pdf. ^ Back to section

154 Page 18 of the MCIT's 2022 Annual Report: https://www.mcit.gov.sa/sites/default/files/2023-07/MCIT_Annual%20Report_2022_En-Web_0.pdf. ^ Back to section

155 Page 51 of the MCIT's 2022 Annual Report: https://www.mcit.gov.sa/sites/default/files/2023-07/MCIT_Annual%20Report_2022_En-Web_0.pdf. ^ Back to section

156 https://www.cst.gov.sa/en/mediacenter/pressreleases/Pages/2020111502.aspx. ^ Back to section

157 https://www.my.gov.sa/wps/portal/snp/content/news/newsDetails/CONT-news-020220222/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfljo8zivQIsTAwdDQz9LQwCXQ0CnV0MfYyNQgwM_M30g1Pz9L30o_ArAppiVOTr7JuuH1WQWJKhm5mXlq8f4ezvF6Kbl1perGtgZGAEQkb6Bdnu4QBP02NO/. ^ Back to section

LATHAM & WATKINS LLP

Brian Meenagh	brian.meenagh@lw.com
Ksenia Koroleva	ksenia.koroleva@lw.com
Danielle van der Merwe	danielle.vandermerwe@lw.com
Faisal Imam	Faisal.Imam@lw.com
Fady Saleh	fady.saleh@lw.com

Latham & Watkins LLP