

THE TECHNOLOGY,  
MEDIA AND  
TELECOMMUNICATIONS  
REVIEW

TWELFTH EDITION

Editor  
Matthew T Murchison

THE LAWREVIEWS

THE

# TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

TWELFTH EDITION

Reproduced with permission from Law Business Research Ltd

This article was first published in December 2021

For further information please contact [Nick.Barette@thelawreviews.co.uk](mailto:Nick.Barette@thelawreviews.co.uk)

**Editor**

Matthew T Murchison

THE LAWREVIEWS

PUBLISHER

Clare Bolton

HEAD OF BUSINESS DEVELOPMENT

Nick Barette

TEAM LEADERS

Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS

Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD

Kieran Hansen

EDITORIAL COORDINATOR

Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR

Adam Myers

PRODUCTION EDITOR

Anne Borthwick

SUBEDITOR

Claire Ancell

CHIEF EXECUTIVE OFFICER

Nick Brailey

Published in the United Kingdom

by Law Business Research Ltd, London

Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

© 2021 Law Business Research Ltd

[www.TheLawReviews.co.uk](http://www.TheLawReviews.co.uk)

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at November 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above.

Enquiries concerning editorial content should be directed  
to the Publisher – [clare.bolton@lbresearch.com](mailto:clare.bolton@lbresearch.com)

ISBN 978-1-83862-834-5

Printed in Great Britain by

Encompass Print Solutions, Derbyshire

Tel: 0844 2480 112

# ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANANTLAW

BAGUS ENRICO AND PARTNERS

BAKER MCKENZIE

CEDAR WHITE BRADLEY

CLEARY GOTTlieb STEEN & HAMILTON LLP

CMS RUSSIA

ELVINGER HOSS PRUSSEN

LATHAM & WATKINS LLP

LEE AND LI, ATTORNEYS-AT-LAW

MLL MEYERLUSTENBERGER LACHENAL FRORIEP AG

RÍOS FERRER, GUILLÉN-LLARENA, TREVIÑO Y RIVERA, SC

SHAHID LAW FIRM

SORAINEN

THE LAW OFFICE OF SALMAN M AL-SUDAIRI

TRAPLE KONARSKI PODRECKI & PARTNERS

URÍA MENÉNDEZ

WEBB HENDERSON

ZHONG LUN LAW FIRM

# CONTENTS

PREFACE.....	vii
<i>Matthew T Murchison</i>	
LIST OF ABBREVIATIONS.....	ix
Chapter 1 AUSTRALIA.....	1
<i>Angus Henderson and Irene Halforty</i>	
Chapter 2 BELARUS.....	37
<i>Kirill Laptev and Pavel Lashuk</i>	
Chapter 3 CHINA.....	50
<i>Jihong Chen</i>	
Chapter 4 COLOMBIA.....	64
<i>Carolina Pardo, Daniela Huertas and Daniel Fajardo</i>	
Chapter 5 EGYPT.....	76
<i>Tarek Badawy, Salma Abdelaziz and Hoda ElBeheiry</i>	
Chapter 6 ESTONIA.....	90
<i>Mihkel Miidla, Liisa Maria Kuuskmaa and Oliver Kuusk</i>	
Chapter 7 FRANCE.....	113
<i>Myria Saarinen and Jean-Luc Juban</i>	
Chapter 8 GERMANY.....	132
<i>Joachim Grittmann and Alexander Wilhelm</i>	
Chapter 9 INDIA.....	147
<i>Rahul Goel, Anu Monga, Saudamini Sharma and Namrata Raj</i>	

## Contents

---

Chapter 10	INDONESIA.....	169
	<i>Enrico Iskandar, Alwin Widyanto Hartanto and Hadyan Farizan</i>	
Chapter 11	ITALY.....	181
	<i>Marco D'Ostuni, Marco Zotta and Riccardo Tremolada</i>	
Chapter 12	JAPAN.....	220
	<i>Stuart Beraha, Hiroki Kobayashi and Benjamin Han</i>	
Chapter 13	LATVIA.....	247
	<i>Andris Tauriņš, Gunvaldis Leitens and Lūcija Strauta</i>	
Chapter 14	LITHUANIA.....	267
	<i>Stasys Drazdauskas</i>	
Chapter 15	LUXEMBOURG.....	278
	<i>Linda Funck</i>	
Chapter 16	MEXICO.....	306
	<i>Ricardo Ríos Ferrer, María Fernanda Palacios Medina and Sonia Cancino Peralta</i>	
Chapter 17	POLAND.....	318
	<i>Xawery Konarski</i>	
Chapter 18	RUSSIA.....	330
	<i>Maxim Boulba and Elena Andrianova</i>	
Chapter 19	SAUDI ARABIA.....	343
	<i>Brian Meenagh, Alexander Hendry, Homam Khoshaim, Lucy Tucker and Avinash Balendran</i>	
Chapter 20	SPAIN.....	365
	<i>Pablo González-Espejo</i>	
Chapter 21	SWITZERLAND.....	386
	<i>Lukas Bühlmann, Michael Reinle and Damian George</i>	
Chapter 22	TAIWAN.....	401
	<i>Ken-Ying Tseng, Vick Chien and Sam Huang</i>	
Chapter 23	UNITED ARAB EMIRATES.....	413
	<i>Fiona Robertson</i>	

## Contents

---

Chapter 24	UNITED KINGDOM.....	420
	<i>Gail Crawford, David Little and Lisbeth Savill</i>	
Chapter 25	UNITED STATES.....	447
	<i>Matthew T Murchison, Elizabeth R Park and Michael H Herman</i>	
Appendix 1	ABOUT THE AUTHORS.....	471
Appendix 2	CONTRIBUTORS' CONTACT DETAILS.....	493

# PREFACE

This volume marks the 12th edition of *The Technology, Media and Telecommunications Review*, which has been fully updated to provide an overview of evolving legal and policy activity in this arena across 25 jurisdictions around the world. This publication continues to occupy a unique space in the literature on TMT issues. Rather than serving a traditional legal treatise, this Review aims to provide a practical, business-focused survey of these issues, along with insights into how this legal and policy landscape in the TMT arena continues to evolve from year to year.

In 2021, the ongoing covid-19 pandemic has continued to loom large over legal and policy developments in this sector. As the threat of infection has continued to affect how we live, work and interact, the importance of connectivity has never been greater or more obvious. For many businesses, remote working has been the rule rather than the exception since March 2020, and may well persist in some form well after the pandemic is over. Many schools switched to distance learning formats during the pandemic. Tele-health is on the rise as doctors check in on patients via videoconference. Even tasks as mundane as grocery shopping have shifted online. And broadband connectivity, where available, has made it all possible.

The experience of covid-19 has, in turn, continued to reshape policymakers' understanding of the TMT arena. The shift to remote working and distance learning has stress-tested broadband networks across the world – providing a 'natural experiment' for determining whether existing policies have yielded robust systems capable of handling substantial increases in internet traffic. At the same time, the pandemic has prompted new initiatives to ensure, improve and expand broadband connectivity for consumers going forward. In various jurisdictions, policymakers are moving forward with subsidy programmes and other efforts to spur the deployment of advanced networks more deeply into unserved and underserved areas. Regulators also have taken steps to preserve internet access where it already exists, including by exploring mandates prohibiting disconnection of customers or requiring certain rates for low-income consumers – measures that, where adopted, sometimes have sparked fresh legal challenges and policy debates over the relative merits of government intervention and market-based solutions.

New technologies likewise have required new approaches and perspectives of policymakers. A notable example is the ongoing deployment of 5G wireless networks, as regulators continue to look for ways to facilitate such deployment. These initiatives take a variety of forms, and frequently include efforts to free up more spectrum resources, including by adopting new rules for sharing spectrum and by reallocating spectrum from one use to another. Multiple jurisdictions have continued to auction off wireless licences in bands newly designated for 5G deployment, capitalising on service providers' strong demand for

expanded access for spectrum. The planned deployment of new satellite broadband services, including multiple large satellite constellations in low-earth orbit, also continues to be a focus of regulatory interest across the world.

Meanwhile, long-running policy battles over the delivery of content over broadband networks continue to simmer in various jurisdictions, and new fronts have opened on related issues involving the content moderation policies of social media companies and other online platforms. Policymakers continue to grapple with questions about network neutrality, the principle being that consumers should benefit from an ‘open internet’ where bits are transmitted in a non-discriminatory manner, without regard for their source, ownership or destination. While the basic principle has been around for well over a decade, unresolved issues remain, including whether newer kinds of network management practices implicate such concerns, and whether efforts to promote a healthy internet ecosystem are best served by light-touch, market-based regimes or by more intrusive government interventions. In the United States, the light-touch approach reinstated in 2018 seems fairly certain to be revisited at the federal level, and certain states are continuing to claim an ability to impose their own restrictions on internet service providers. Regulators around the world have begun taking more aggressive enforcement action against internet service providers’ zero rating plans, which exempt certain data from counting against a customer’s usage allowance. Regulators in Asia are grappling with similar policy questions. In addition, these neutrality principles, usually debated in the context of broadband networks, are now spilling over to the content side, where social media companies are facing increased scrutiny over claims of discriminatory practices in moderating content appearing on their platforms. Indeed, some jurisdictions are considering measures that not only would rescind immunities these platforms have traditionally enjoyed for their content moderation practices, but also would require increased transparency and potentially even impose anti-discrimination mandates or other consumer protections. In short, while the balance of power between broadband network operators and online content providers historically has turned on the degree of regulation of the former, both sides’ practices are now very much in the spotlight.

The following country-specific chapters describe these and other developments in the TMT arena, including updates on privacy and data security, regulation of traditional video and voice services, and media ownership. On the issue of foreign ownership in particular, communications policymakers have increasingly incorporated national security considerations into their decision-making.

Thanks to all of our contributors for their insightful contributions to this publication. I hope readers will find this 12th edition of *The Technology, Media and Telecommunications Review* as helpful as I have found this publication each year.

**Matthew T Murchison**

Latham & Watkins LLP

Washington, DC

November 2021

# SAUDI ARABIA

*Brian Meenagh, Alexander Hendry, Homam Khoshaim, Lucy Tucker and Avinash Balendran<sup>1</sup>*

## I OVERVIEW

The year 2021 saw significant further developments to the technology, media and telecommunications regulatory regime in Saudi Arabia with new laws and regulatory bodies emphasising the importance of this sector to Saudi Arabia's Vision 2030 programme.<sup>2</sup>

In particular, we have seen a new national privacy law (as we predicted in the previous edition's chapter), a draft media law and updates to the CITC cloud computing regulatory framework. We expect further regulatory evolution over the next few years.

This chapter provides an overview of technology, media, telecommunications and data regulation in Saudi Arabia. Given the wide scope of the subject matter, 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.

## II REGULATION

### i The regulators

The technology and telecommunications sector in Saudi Arabia is principally regulated by two bodies: the Ministry of Communications and Information Technology (MCIT)<sup>3</sup> (formerly, the Ministry of Post, Telegraph and Telephone) and the Communications and Information Technology Commission (CITC).

A small number of other authorities have more discrete remits. Recently, Saudi Arabia has expanded regulation into the field of cybersecurity, which has led to the creation of the National Cybersecurity Authority (NCA).<sup>4</sup> Pursuant to Article 2 of the NCA Bylaws, the NCA enjoys financial and administrative independence, and reports to the King directly. Article 5 of the NCA Bylaws provides that the NCA may establish affiliate centres to carry out some of its responsibilities and tasks. On that basis, the NCA has established the National Cyber Security Center (NCSC) and Saudi CERT.

The key regulators for media and media protection in Saudi Arabia are the Ministry of Media (MoM)<sup>5</sup> and General Commission for Audiovisual Media (GCAM).<sup>6</sup>

---

1 Brian Meenagh is a partner and Alexander Hendry, Lucy Tucker and Avinash Balendran are associates at Latham & Watkins LLP. Homam Khoshaim is an associate at the Law Office of Salman M Al-Sudairi.

2 <https://vision2030.gov.sa/en>.

3 <https://www.mcit.gov.sa/en>.

4 <https://nca.gov.sa/en/index.html>.

5 <https://www.media.gov.sa/en>.

6 <https://www.gcam.gov.sa/en>.

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 CITC is responsible for issuing licences in accordance with the Telecom Act and implementing approved plans and programmes for the supervision and management of the technology and telecommunications sector. Decisions made by the CITC can be appealed to MCIT.

#### *Other relevant regulators*

- a* The Saudi Authority for Data and AI (SDAIA): the 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.<sup>7</sup>
- b* The National Centre for Digital Certification (NCDC): 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).<sup>8</sup>
- c* The National Digital Transformation Unit (NDTU): established in 2017, the NDTU 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.<sup>9</sup>
- d* The Saudi Authority for Intellectual Property (SAIP): established in 2018 with the aim of organising, supporting, sponsoring, protecting and promoting intellectual property in Saudi Arabia in accordance with global best practices.<sup>10</sup>

#### *Cybersecurity regulators*

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

- a* achieving security and stability, providing safety for Saudi Arabia citizens and protection against crime;

---

7 <https://sdaia.gov.sa/>.

8 <https://www.ncdc.gov.sa/?lang=en>.

9 <https://ndu.gov.sa/en/>.

10 <https://www.saip.gov.sa/en/>.

- b* reinforcing security relationships with neighbouring Arab and GCC countries, to maintain safety in Saudi Arabia and abroad, to control crime and drug smuggling, and exchange security information; and
- c* 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.<sup>11</sup> Prosecutions are led by the Bureau of Investigation and Prosecution.

The NCA was established by royal decree in October 2017 as the body responsible for the protection and promotion of cybersecurity matters in Saudi Arabia. In October 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)<sup>12</sup> and Cloud Cybersecurity Controls (CCC – 1: 2020).<sup>13</sup>

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 in order to safeguard its vital interests, national security, critical infrastructure, high-priority sectors and government services and activities in alignment with Vision 2030. The NCA also oversees the NCSC and Saudi CERT. The NCSC has a national role in monitoring and analysing cyber risks and threats, and sharing information with government entities and critical national infrastructures. Saudi CERT's primary mission is to raise cybersecurity awareness in Saudi Arabia.

### ***Media***

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

GCAM is responsible for the regulation of audiovisual media transmission in Saudi Arabia. It reports to the MoM but is a separate legal entity with independent finance and administration.

## **ii Main sources of law**

### ***Technology and telecommunications***

- a* 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).<sup>14</sup>
- b* The Communication and Information Technology Commission Ordinance (CITC Ordinance) (issued under the Council of Ministers resolution No. (74), dated

---

11 See <https://www.saudi.gov.sa/wps/portal/snp/individuals/servicedetails/6166> for further information.

12 <https://nca.gov.sa/en/pages/ecc.html>.

13 <https://nca.gov.sa/files/ccc-en.pdf>.

14 [https://www.citc.gov.sa/en/RulesandSystems/CITCSysstem/Documents/LA%20\\_001\\_E\\_%20Telecom%20Act%20English.pdf](https://www.citc.gov.sa/en/RulesandSystems/CITCSysstem/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf).

05/03/1422H (corresponding to 27/05/2001), and amended pursuant to the Council of Ministers resolution No. (133), dated 21/05/1424H (corresponding to 21 July 2003).<sup>15</sup>

c The E-Commerce Law 2019 (Royal Decree No. M/126 dated 07/11/1440H (corresponding to 10 July 2019)).<sup>16</sup>

The CITC's role has expanded beyond telecommunications and it has issued a variety of regulations and consultations<sup>17</sup> in a number of sectors in the technology and digital space, including:

- a the Cloud Computing Regulatory Framework (version 3, which came into effect on 18/04/1442 H (corresponding to 3 December 2020)) (Cloud Regulations): the Cloud Regulations outline the rights and obligations of cloud service providers (CSPs) and users of cloud services (i.e., cloud customers); they only apply to CSPs who are based in Saudi Arabia or have customers based in Saudi Arabia;<sup>18</sup>
- b the Regulation for the Reduction of Spam (Spam Regulations): the Spam Regulation 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;
- c CITC Decision No. 395/1439 dated 3/11/1439H (corresponding to 14 August 2018);<sup>19</sup>
- d the Internet of Things Regulatory Framework, issued in September 2019;<sup>20</sup>
- e Rules and Conditions for MVNO Services and IoT-VNO Services Provision: these update the conditions and licensing requirements related to the request for a licence to provide mobile virtual network operator services. They set out the conditions and licensing requirements relating to the provision of the services by internet of things virtual network operators;<sup>21</sup>
- f the Saudi Domain Name Registration Regulation<sup>22</sup> and related guidelines and rules;<sup>23</sup>
- g the regulations, guidelines and rules for the registration of Saudi country-code top-level domains. They are issued by the Saudi Network Information Centre (SaudiNIC),<sup>24</sup> part of the CITC; and

15 [https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA\\_002\\_E\\_CITC%20Ordinance.pdf](https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_002_E_CITC%20Ordinance.pdf).

16 An English translation is not yet available.

17 <https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/default.aspx>.

18 [https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF\\_En.pdf](https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf).

19 [https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/ReductionofSPAM/Documents/IT%20008%20E%20-%20Regulation\\_For\\_The\\_Reduction\\_of\\_SPAM\\_Eng.pdf](https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/ReductionofSPAM/Documents/IT%20008%20E%20-%20Regulation_For_The_Reduction_of_SPAM_Eng.pdf).

20 [https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT\\_REGULATORY\\_FRAMEWORK.pdf](https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf).

21 <https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Licenses/LicensingRegulatoryFrameworks/Documents/PL-SP-021-A-MVNO-EN.pdf>.

22 <https://www.nic.sa/en/view/regulation>.

23 <https://nic.sa/en/cat/rules>.

24 <https://www.nic.sa/en/>.

- b* the Rules and Technical Standards for ICT Infrastructure Deployment in New Developments: these are intended to facilitate the implementation and rollout of telecom networks.<sup>25</sup>

Additional regulatory documents issued by CITC relating to the technology and telecoms sector can be found on the CITC website.<sup>26</sup>

### *Cybersecurity*

The key relevant cybersecurity laws are as follows:

- a* Royal Decree No. 5/11/8697 dated 26/8/1370 H (corresponding to 2 June 1951) (Law Establishing the Ministry of Interior);
- b* the Anti-Cyber Crime Law (issued under the Council of Ministers Decision No. 79, dated 7/3/1428 H (corresponding to 26 March 2007), and approved by Royal Decree No. M/17, dated 8/3/1428 H (corresponding to 27 March 2007) (Cyber Law);<sup>27</sup> and
- c* the Cloud Regulations.

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).

### *Privacy*

In September 2021, a new Personal Data Protection Law (PDPL) was issued (pursuant to Cabinet Resolution No. 98 of 7/2/1443H and Royal Decree M/19 of 9/2/1443H). The PDPL will come into force in March 2022. The PDPL delegates a lot of matters to the Executive Regulations, which are to be issued by the Competent Authority, namely the SDAIA (for at least the next two years), 180 days after the issuance of the PDPL (just before the PDPL comes into force).

### *Media*

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

- a* the Publications Law promulgated by Royal Decree No. M/32 dated 03/09/1421H (corresponding to 29 November 2000);
- b* the Electronic Publications Regulations published on 20/04/1432H (corresponding to 25 March 2011);
- c* the Press Institutions Law promulgated by Royal Decree No. M/20 dated 08/05/1422H (corresponding to 29 July 2001) (Press Institutions Law);
- d* the General Commission for Audiovisual Media Regulations promulgated by Royal Decree number 33/M dated 25/03/1439H (corresponding to 13 December 2017) (GCAM Regulations);
- e* the GCAM Implementing Regulations promulgated by Minister of Media resolution No. 16927 dated 04/03/1440H (corresponding to 12 November 2018) (GCAM Implementing Regulations); and

---

25 <https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/ICTInfrastructure.aspx>.

26 <https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/default.aspx>.

27 [https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA\\_004\\_%20E\\_%20Anti-Cyber%20Crime%20Law.pdf](https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf).

- f* the Copyright Law promulgated by Royal Decree No. M/41 dated 02/07/1424H (corresponding to 30 August 2003).

GCAM announced a Draft Media Law for public consultation on 29/12/1441H (corresponding to 19 August 2020). Once it comes into effect following publication of the Regulations in the Official Gazette, it will replace the GCAM Regulations and the Publications Law.

#### *Publications and press institutions*

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

- a* the Law of Printing and Publication and its implementing regulations, regulating print and publication activities; and
- b* the Implementing Regulations for Electronic Publishing, regulating the practice of electronic publishing in Saudi Arabia.

#### *Audiovisuals*

For the implementation of media laws in relation to audiovisuals, the GCAM has issued the implementing regulations governing the following matters:

- a* importing and selling receivers;<sup>28</sup>
- b* licensing visual and audible media content production companies;<sup>29</sup>
- c* establishing a representative offices of TV channels;<sup>30</sup>
- d* importing, distributing, selling and renting visual and audible media content;<sup>31</sup>
- e* establishing studios;<sup>32</sup>
- f* audiovisual broadcasting services over telecommunication networks;<sup>33</sup>
- g* TV and radio competitions;<sup>34</sup>
- h* satellite news gathering (SNG) services;<sup>35</sup>
- i* audio social communication services;<sup>36</sup>

---

28 <http://ncar.gov.sa/Documents/Details?Id=FcuO0O65mqv6hUJyQTqGoQ%3D%3D>. An English translation is not yet available.

29 <http://ncar.gov.sa/Documents/Details?Id=1MYbzcTWDtG73jvEANK3PQ%3D%3D>. An English translation is not yet available.

30 <http://ncar.gov.sa/Documents/Details?Id=hd7cqmBdRYV1%2BtMCCV63%2Bg%3D%3D>. An English translation is not yet available.

31 <http://ncar.gov.sa/Documents/Details?Id=H72YTNxW3IS3MwUvEYZEa%3D%3D>. An English translation is not yet available.

32 <http://ncar.gov.sa/Documents/Details?Id=I9s%2BthH2KdfE7gG%2FG4b8WQ%3D%3D>. An English translation is not yet available.

33 <http://ncar.gov.sa/Documents/Details?Id=kC0xTcvz6I6QmCgfWZN5uw%3D%3D>. An English translation is not yet available.

34 <http://ncar.gov.sa/Documents/Details?Id=W5xSXAHO2ElvFCmaJWltzg%3D%3D>. An English translation is not yet available.

35 <http://ncar.gov.sa/Documents/Details?Id=RDTW06ZGhCgAlfarI62%2FTw%3D%3D>. An English translation is not yet available.

36 <http://ncar.gov.sa/Documents/Details?Id=nIWrewmfgu7D5ZyZWtZDQg%3D%3D>. An English translation is not yet available.

- j* visual broadcasting via closed circuit services;<sup>37</sup>
- k* on-demand video services issued by the GCAM;<sup>38</sup> and
- l* videogame participation.<sup>39</sup>

### **iii Regulated activities**

Generally, each relevant regulator maintains its processes for issuing its licences pursuant to its own regulations, rules and policies. However, more regulators are adopting the use of a unified e-licence issuing system named 'Meras'.<sup>40</sup> Meras allows applicants to submit online applications to obtain licences issued by regulators participating in the Meras platform. We expect that any remaining licences requiring in-person attendance will be phased out in favour of online submissions, either through the relevant regulator or through the Meras platform.

### ***Technology***

The Telecom Act provides a legal foundation for supervising and managing the telecommunications sector in Saudi Arabia. It also outlines certain objectives for the sector. These include:

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

Any entity seeking to provide telecommunications services must submit a licence application to the CITC.

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

---

37 <http://ncar.gov.sa/Documents/Details?Id=N8zzTS1L9PIVRyIvZKih7Q%3D%3D>. An English translation is not yet available.

38 <http://ncar.gov.sa/Documents/Details?Id=0bYan%2FrPjGJntHUNchtwcQ%3D%3D>. An English translation is not yet available.

39 <http://ncar.gov.sa/Documents/Details?Id=1DpjOttTK1WQLvDHIDHzg%3D%3D>. An English translation is not yet available.

40 <https://meras.gov.sa/en/about/>.

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

- a* issuing the necessary licences in accordance with all relevant laws;
- b* ensuring the implementation of the conditions specified in such licences;
- c* implementing approved policies, plans and programmes for developing the telecommunications sector;
- d* achieving the orderly expansion of the telecommunications infrastructure and telecommunications services provided to the users in an effective and reliable manner; and
- e* encouraging reliance on market forces for the provision of telecommunication services.

### *Cybersecurity*

CSPs that exercise direct or effective control over data centres or critical cloud infrastructure hosted in Saudi Arabia are required to register with the CITC.

### *Privacy*

Under Article 32 of the PDPL, controlling entities are required to register on a national portal and the Competent Authority may impose a registration fee of up to 100,000 riyals per year for the registration.

## **Media**

### *Publications*

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

- a* print, publish or distribute publications or engage in any other publication services;
- b* import, sell or rent movies or video tapes;
- c* produce, sell or rent computer programs;
- d* engage in any press services; and
- e* 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 in order to carry out electronic publication. Such 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 in order 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 the GCAM, the approval of the Council of Ministers is required based on the recommendation of GCAM.

There are three types of licences that can be obtained from GCAM: media activity licenses, cinema licences and broadcasting and distribution licences.

#### **iv 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. However, we note that 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.

#### **v 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.<sup>41</sup> From an operational perspective and depending on the type of licence, the requirements for licences transfers may range from no action required, notification to the relevant regulator, to obtaining regulator consent (including re-application). We note that the General Authority for Competition has recently 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.<sup>42</sup>

### **III TELECOMMUNICATIONS AND INTERNET ACCESS**

#### **i 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. We note for example that the Ministry of Human Resources and Social Development has implemented a ministerial decision that was announced on 5 October 2020 and has come into effect on 27 June 2021 for Saudisation of a number of occupations within the telecommunications field.<sup>43</sup>

---

41 [https://gac.gov.sa/index\\_en.asp](https://gac.gov.sa/index_en.asp).

42 [https://www.linkedin.com/posts/talal-alhoggail-m-a-000a6a116\\_merger-review-guidelines-ugcPost-6848551624420450304-B0QD](https://www.linkedin.com/posts/talal-alhoggail-m-a-000a6a116_merger-review-guidelines-ugcPost-6848551624420450304-B0QD).

43 <https://hrsd.gov.sa/sites/default/files/5102020.pdf>.

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 Regulations as well as the various regulations issued by the CITC and referred to above.

## ii Universal service

Saudi Arabia has encouraged the development of telecom and broadband infrastructure and adopted the same under its Vision 2030. Prior to the strategies adopted under Vision 2030, the CITC issued the Universal Access and Universal Service Policy<sup>44</sup> (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.<sup>45</sup> According to the CITC, 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.<sup>46</sup>

## iii Restrictions on the provision of service

Service providers are regulated broadly under the Telecom Act.

In addition, the CITC has revised its relevant regulations concerning the rights, obligations and terms of ICT service providers and users (Amended Service Providers Regulations)<sup>47</sup> 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 CITC 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, provided that such information must include the following at a minimum:

- a* clarifications about the method of subscription and cancellation mechanisms;
- b* types of calls available in the package being purchased or advertised;
- c* the number of minutes granted for each type of call available in the package;
- d* types of calls excluded from the package;
- e* the mechanism for dealing with minutes, data amount or remaining balance;
- f* the validity or expiry of remaining balance;
- g* an explanation as to the number of minutes or amount of data available, or both, and information about use during or outside peak periods;
- h* penalty conditions, if any;
- i* provision of the service in the event of implementation of restrictions on use in terms of quality and availability;
- j* cases in which usage restrictions apply;
- k* any limitations or restrictions on usage that would affect use of the service;

---

44 [https://www.citc.gov.sa/en/RulesandSystems/bylaws/Documents/LA%20007\\_%20%20E\\_%20%20The%20Universal%20Access%20and%20Universal%20Service%20Policy.pdf](https://www.citc.gov.sa/en/RulesandSystems/bylaws/Documents/LA%20007_%20%20E_%20%20The%20Universal%20Access%20and%20Universal%20Service%20Policy.pdf).

45 Article 1 of the Universal Access and Universal Service Policy.

46 <https://www.citc.gov.sa/en/USF/Pages/Projects.aspx>.

47 [https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/Documents/Termstelecomservices\\_en.pdf#search=service%20providers%20regulations](https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/Documents/Termstelecomservices_en.pdf#search=service%20providers%20regulations).

- l* necessary means for users to enable them to follow up on their usage; and
- m* information related to the mechanism for applying a settlement with the user in case the service provider is unable to meet the quality standards approved by the CITC 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. Even so, such telemarketing must be in accordance with the following:

- a* contact must be through official communication channels only;
- b* communication must be recorded;
- c* the user's identity must be verified;
- d* 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
- e* 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 CITC.

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 has been provided with a notice of the expiry date at least 24 hours in advance; and (2) the user has 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 CITC.

Under the Amended Service Providers Regulations, all user information is considered confidential and service providers are obliged to maintain such 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 CITC. 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 such 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.

#### **iv 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 relating to individuals residing in Saudi Arabia, by entities outside of Saudi Arabia.<sup>48</sup> 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 significant differences. Key legal requirements to note include:

- a* under Article 5, consent is the primary legal basis for processing, and the only legal basis relating to marketing.<sup>49</sup> The Executive Regulations will set out the conditions of consent and cases in which consent must be in writing. The PDPL does not contain a legitimate interests of the data controller or a third party legal basis for processing personal data, which is a key business-friendly lawful basis relied on in other privacy regimes;
- b* under Article 29, there is a general restriction on transferring personal data outside of Saudi Arabia, unless in cases of extreme necessity to preserve life of the data owner, in the vital interests of the data owner or to treat an infection. For all other transfers, there is no concept of 'adequate jurisdictions' or other means of transferring personal data outside of Saudi Arabia (such as standard contractual clauses) and a transfer may only occur for limited purposes (e.g., to serve the interests of Saudi Arabia), provided that the transfer does not prejudice national security or the interests of Saudi Arabia, sufficient guarantees are provided relating to confidentiality, only minimal personal data is transferred, and the Competent Authority has approved the transfer;
- c* under Articles 12 and 13, controlling entities must provide individuals with information on the data processing; and
- d* under Article 20(1), a controlling entity is required to notify the Competent Authority 'as soon as it becomes aware' of the occurrence of a leakage to or damage of personal data or illegal access thereto, and under Article 20(2), if a data breach would cause 'serious harm' to the individual then the controlling entity must notify the individual 'immediately'.

Key administrative provisions include:

- a* under Article 31, controlling entities are required to maintain a record of their processing activities and make these available to the Competent Authority on request;
- b* under Article 32, controlling entities are required to register on a national portal and the Competent Authority may impose a registration fee of up to 100,000 riyals per year for the registration;
- c* under Article 30(2), controlling entities must appoint one or more employees to be responsible for its commitment to implement data protection requirements; and

---

48 Article 2(1).

49 Article 25.

- d* under Article 33(2), entities outside Saudi Arabia that are within scope of the PDPL are required to appoint a local representative in Saudi Arabia.

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

- a* under Article 35(1)(a), disclosure of sensitive data in breach of the PDPL may result in up to two years' imprisonment or up to a 3 million riyal fine, or both;
- b* under Article 35(1)(b), transfer of data outside of Saudi Arabia in breach of the PDPL may result in up to one year's imprisonment or up to a 1 million riyal fine, or both;
- c* under Article 36, all other matters of noncompliance may result in a warning or a fine of up to 5 million riyals, which is doubled for repeat offences; and
- d* under Article 40, individuals can make compensation claims for material or moral damage.

The PDPL follows the issuance of National Governance Interim Regulations (Interim Regulations) published by the NDMO on 1 June 2020.<sup>50</sup> The Interim Regulations contain interim regulations on the following topics:

- a* data classification, which applies to all data received, produced or managed by public entities;
- b* 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 related to individuals residing in Saudi Arabia, by any means;
- c* data sharing, which applies to the sharing of government data with other public entities, private entities and individuals;
- d* freedom of information, which applies to requests from individuals to access or obtain unprotected public information produced or held by public entities; and
- e* open data, which applies to all unprotected data and public information produced by public entities.

Although not identical, the Personal Data Protection Interim Regulations cover a number of the same areas as the PDPL, including data protection principles, the rights of individuals and controller obligations. Although the PDPL does not specifically repeal the Interim Regulations, it is expected that the PDPL will take precedence for privacy matters, to the extent they are also addressed in the Interim Regulations (i.e., on Personal Data Protection), and the Executive Regulations issued under the PDPL may provide further guidance and direction on this.

Unlike the PDPL, the Interim Regulations do not contain any express enforcement mechanisms or penalties for noncompliance.

Prior to the PDPL and Interim Regulations, Saudi Arabia did not have a comprehensive data protection law, and the primary source of data protection law were Sharia principles (i.e., Islamic principles derived from the Holy Quran and the Sunnah), a number of rights that protect privacy in the Basic Law of Governance 1992 (Royal Order No. A/91 of 1992) (Basic Law)<sup>51</sup> and sectorial legislation.

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

---

50 <https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf>.

51 <https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/16b97fcb-4833-4f66-8531-a9a700f161b6/1>.

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 is:

- a* 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 CITC has published ‘procedures for launching services or products based on customers’ personal data, or sharing personal data’,<sup>52</sup> which contain a requirement to conduct a privacy impact assessment and submit this to the CITC 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;
- b* related legislation that contains data protection obligations, for example, the Cloud 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;<sup>53</sup> and
- c* 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 Personal Data Protection Act BE 2562 (2019)).

Regarding the processing of children’s’ data, on 25 November 2020, the NDMO published a Children’s and Incompetents Privacy Protection Policy,<sup>54</sup> 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.

In addition to the discussion in Section II.i 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.

## **v Freedom of expression**

Article 8 of the Publications Law (and Article 8 of the Draft Media Law) also guarantees freedom of expression in different forms of publication.<sup>55</sup>

---

52 <https://www.citc.gov.sa/en/RulesandSystems/privacy/Documents/Procedures-data-privacy-en.pdf>.

53 [https://www.citc.gov.sa/en/RulesandSystems/CITCSysstem/Documents/LA\\_004\\_%20E\\_%20Anti-Cyber%20Crime%20Law.pdf](https://www.citc.gov.sa/en/RulesandSystems/CITCSysstem/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf).

54 <https://sdaia.gov.sa/ndmo/Files/Policies002.pdf>.

55 <https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/eccaec43-8ff9-46b8-b269-a9a700f16e66/2>.

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):

- a* 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; and
- b* 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.
- c* 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’, ‘destabilizing national security or state stability’, ‘endangering national unity’ and ‘suspending the basic laws of governance’, all of which may encompass any form of expression.<sup>56</sup>

## **IV SPECTRUM POLICY**

### **i Development**

The following pieces of legislation regulate this area:

- a* The Telecom Act: the regulation of radio spectrum usage is one of the main functions of the CITC 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.
- b* The National Spectrum Strategy 2025: the CITC has recently published a National Spectrum Strategy 2025<sup>57</sup> that describes the CITC’s priorities with respect to the development of Saudi Arabia’s spectrum policy going forward. The Spectrum Strategy states that Saudi Arabia has already achieved considerable success in assigning spectrum to public mobile networks that utilise International Mobile Telecommunication

---

<sup>56</sup> ‘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 such 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.

<sup>57</sup> [https://www.citc.gov.sa/ar/services/spectrum/Documents/National%20Spectrum%20Strategy\\_E.pdf](https://www.citc.gov.sa/ar/services/spectrum/Documents/National%20Spectrum%20Strategy_E.pdf).

standards to provide mobile broadband services, and notes the creation of a dedicated subcommittee in 2019 under the auspices of the CITC to focus on 5G spectrum matters within the National 5G Taskforce.

## **ii Flexible spectrum use**

Under the Spectrum Strategy, a comprehensive review of fixed point-to-point links is contemplated in order 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 Telecommunication (IMT) field, which resulted in the country's ranking among the leading nations in awarded IMT spectrum. In March 2021, the CITC issued a plan for the allocation and use of spectrum bands identified for IMT (IMT Spectrum Plan),<sup>58</sup> which aims 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 CITC to work on satellite coordination requests and resolve such requests in a timely manner, thereby allowing existing and future satellite services access to spectrum and manage trade-offs with IMT allocations.

## **iii 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 others, 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 in order to position Saudi Arabia among the leading nations in unlocking innovative high-performance use cases and applications based on 5G.

## **iv Spectrum auctions and fees**

### ***Auctioning spectrum***

As of the third quarter of 2020, the CITC has auctioned spectrum to licensed mobile networks operators within Saudi Arabia.

In 2017, the CITC 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).<sup>59</sup> This was the first spectrum auction in Saudi Arabia and the first time spectrum in the 700MHz band has been 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.

---

58 <https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/FrequencySpectrum/Documents/SM-Regulation%20and%20Allocation%20for%20Spectrum%20Bands%20Identified%20for%20IMT.pdf>.

59 <https://www.citc.gov.sa/en/MediaCenter/PressReleases/Pages/2017060601.aspx>.

Additionally, the CITC 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 CITC's released statement noted that the CITC 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 the CITC 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 2x5MHz each in the 410–430MHz and 450–480MHz bands either as part of the auction or separately.

The CITC then published a public consultation on 7 October 2021 on an upcoming spectrum auction of 2100MHz for non-terrestrial networks. The CITC 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 CITC's released statement noted that the CITC 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 CITC on its public consultation issued on 30 May of 2021 (referenced above), the CITC has 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. The auction is 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.

### ***Spectrum fees***

Currently, spectrum users must be licensed by the CITC and such licence is accompanied by a fee to be paid to the CITC calculated in accordance with the CITC's Spectrum Fees of Frequency Usage Policy.<sup>60</sup>

## **V MEDIA**

### **i Regulation of media distribution generally**

In addition to the key laws regulating media and media protection specified in Section II.ii, the following laws are also relevant in regulating media and media protection in Saudi Arabia:

- a* the National Committee for Regulating Digital Media Content formed pursuant to a Council of Ministers resolution dated 23/03/1435H (corresponding to 24 January 2014);
- b* the Media Policy in Saudi Arabia issued by the MoM;<sup>61</sup> and
- c* the General Commission for Audiovisual Media age classification guide.

---

60 <https://www.citc.gov.sa/en/RulesandSystems/Bylaws/Pages/FinancialSpectrumPolicy.aspx>.

61 An official English translation is unavailable on the MoM's website.

As above, the Draft Media Law, once it comes into effect, will replace the GCAM Regulations and the Publications Law. As this has not yet 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.

## **ii 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 in the licence manual that accompanies the GCAM Implementing Regulations include:

- a* media content production, and operating media production studios;
- b* advertising agencies;
- c* operating cinemas;
- d* satellite distribution;
- e* terrestrial transmission;
- f* satellite uplink stations;
- g* linear and non-linear (e.g., video on demand and over the top) broadcasting;
- h* radio broadcasting;
- i* IPTV and cable television;
- j* media audience measurement; and
- k* 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 others):

- a* comply with the GCAM's policies with regard to prioritising the use of Kingdom resources, including human resources; and
- b* 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 licenses 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 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 license and the requirement to publish an apology.

### **iii Content restrictions**

Article 9 of the Draft Media Law lists media content that may not be published, which includes any media that prejudices the principles of Islamic Sharia or the supreme interests of Saudi Arabia; threatens national or international peace; instigates the committing of crime or violence, breaches national security, public order, public morals or public health; infringes the rights of others; instigates racism, national or religious hatred; or promotes drugs, alcohol or tobacco. Article 13 requires that media content be submitted to the General Authority for Media Regulation (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 programs 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 10/24/1417 AH prohibits users within Saudi Arabia from publishing or accessing illegal, harmful or anti-Islamic content on the internet.

Previously, the Internet Service Unit operated a data link that connected Saudi Arabia to the international internet. Users would subscribe to any number of local internet service providers and all web traffic would have been forwarded through servers at the Internet Service Unit. The foregoing structure has been modified, and we understand that multiple data service providers act as a proxy between the internet service providers and the international internet. The CITC is now responsible for administering the internet filtering service, which was previously under the Internet Service Unit's domain.

The CITC provides such services in cooperation with the Permanent Internet Security Committee, and provides a list of banned websites to the data service providers.

Alternatively, users may submit a request to block a particular website where they deem such a website or material to contain undesirable content. Once a user has submitted the web-based form, it is reviewed by a team of CITC 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 CITC's instructions, it may result in a fine of up to 5 million riyals.<sup>62</sup>

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 CITC regulates network operators, and the ICT and postal sector. The Telecom Act provides the legal framework for organising this sector.<sup>63</sup>

---

62 Freedom of the Net 2019, Saudi Arabia, Freedom House.

63 <https://www.citc.gov.sa/en/AboutUs/AreasOfwork/Pages/default.aspx>.

The GCAM regulates the audiovisual sector,<sup>64</sup> and the MoM supervises all means of visual, audio and written communication content in Saudi Arabia.<sup>65</sup>

Pursuant to the Publications Law, a licence from the MoM is required to carry out, among other things, the following activities: printing, publishing or distributing publications or engaging in any other publication services; importing, selling or renting movies or video tapes; producing, selling or renting computer programs; engaging in any press services; and carrying out photography services.

The activities mentioned above are restricted to 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 GCAM: media activity licences; cinema licences; and broadcasting and distribution licences. As such, we understand that emerging platforms are more likely to fall within the GCAM Regulations and GCAM Implementing Regulations.

Content restrictions are also imposed under the Cloud Regulations. Article 3.5.2 of the Cloud Regulations states that cloud service providers are not liable for unlawful content or infringing content that has been uploaded, processed or stored on the cloud service providers' systems, and Article 3.5.3 of the Cloud 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 Regulations states that cloud service providers must remove such unlawful or infringing content or render it inaccessible within the country after written notice by the CITC or any other authorised entity, or per Article 3.5.5, may do so on its own initiative or following a third-party request.<sup>66</sup>

In addition, mandatory controls are required for posting adverts on social media platforms, including clearly announcing that the content is an advert,<sup>67</sup> not including false or misleading information or adverts for counterfeit or fraudulent products.<sup>68</sup>

#### **iv Internet-delivered video content**

There is limited information on how the move from broadcast video distribution to internet video distribution has 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 CITC's 2017 Annual Report (which is the latest published to date), the penetration rate of internet services has soared over the past years from 64 per cent in 2014 to around 82 per cent by the end of 2017 and, accordingly, the demand for internet

---

64 <https://www.gcam.gov.sa/>.

65 [https://www.my.gov.sa/wps/portal/snp/pages/agencies/agencyDetails/AC164!/ut/p/z0/04\\_Sj9CPyKssy0xPLMnMz0vMAfJjo8zivQIsTAwdDQz9LQwNzQwCnS0tXPwMvYwNDAz0g1Pz9L30o\\_ArAppiVOTr7JuuH1WQWJkHm5mXlq8f4ehsaGaiX5DtHg4AfoZqHw!!!](https://www.my.gov.sa/wps/portal/snp/pages/agencies/agencyDetails/AC164!/ut/p/z0/04_Sj9CPyKssy0xPLMnMz0vMAfJjo8zivQIsTAwdDQz9LQwNzQwCnS0tXPwMvYwNDAz0g1Pz9L30o_ArAppiVOTr7JuuH1WQWJkHm5mXlq8f4ehsaGaiX5DtHg4AfoZqHw!!!).

66 [https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF\\_En.pdf](https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf).

67 Article 10 of the Implementing Regulations of the E-Commerce Law.

68 Article 12 of the E-Commerce Law.

and broadband services has risen.<sup>69</sup> The CITC's Digital Insights quarterly report for the fourth quarter of 2020 notes that mobile and fixed internet data consumption continues on an upward trajectory, in particular due to the number of smartphone users, increase in data usage during the covid-19 pandemic and the availability of affordable unlimited data packages.<sup>70</sup>

In addition, Saudi Arabia has a 'KSA Free Wifi Initiative',<sup>71</sup> which gives users access to free connectivity in 60,000 WiFi hotspots in public places across Saudi Arabia.

As such, it is reasonable to presume that the move from broadcast video distribution to internet video distribution has not had a significant negative impact on consumers, given the high rate of access to the internet in Saudi Arabia.

## **VI THE YEAR IN REVIEW**

In June 2020, the CITC issued a revised draft of the Amended Service Providers Regulations,<sup>72</sup> which regulates the rights, obligations and terms of ICT service providers and users with the aim to reduce unsolicited calls and messages.

In August 2020, GCAM announced a Draft Media Law for public consultation. Once it comes into effect following publication of the Regulations in the Official Gazette, it will replace the key laws regulating media and media protection (i.e., the GCAM Regulations and the Publications Law).

The CITC issued version 3 of the Cloud Regulations, which came into effect on 18/04/1442H (corresponding to 3 December 2020). The Cloud Regulations outline the rights and obligations of CSPs and users of cloud services. They only apply to CSPs that are based in Saudi Arabia or that have customers based in Saudi Arabia.<sup>73</sup>

In March 2021, the CITC launched the IMT Spectrum Plan,<sup>74</sup> which aims to identify the frequency allocation and use regulations for radio spectrum bands identified for IMT services. The CITC then proceeded to publish the public consultation results relating to spectrum auctions showcasing the commercial promise of spectrum auctioning.

One of the most anticipated sets of regulations was the PDPL, issued in September 2021. The PDPL, which will come into force in March 2022, introduces new data and privacy requirements applicable to any processing of personal data by any means that takes place in Saudi Arabia. However, the PDPL has delegated a lot of matters to the Executive Regulations that are to be issued by the competent authority, namely the SDAIA, 180 days after the issuance of the PDPL.

In February 2021, the NCA issued the final draft of its Cloud Cybersecurity Controls – CCC-1:2020.<sup>75</sup>

---

69 Page 136 of the CITC's 2017 Annual Report: [https://www.citc.gov.sa/en/mediacenter/annualreport/Documents/PR\\_REP\\_013Eng.pdf](https://www.citc.gov.sa/en/mediacenter/annualreport/Documents/PR_REP_013Eng.pdf).

70 <https://www.citc.gov.sa/ar/mediacenter/Documents/DigitalInsights-en20q4.pdf>.

71 <https://www.citc.gov.sa/en/mediacenter/pressreleases/Pages/2020111502.aspx>.

72 [https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/Documents/Termstelecomservices\\_en.pdf#search=service%20providers%20regulations](https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/Documents/Termstelecomservices_en.pdf#search=service%20providers%20regulations).

73 [https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF\\_En.pdf](https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf).

74 <https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/FrequencySpectrum/Documents/SM-Regulation%20and%20Allocation%20for%20Spectrum%20Bands%20Identified%20for%20IMT.pdf>.

75 <https://nca.gov.sa/files/ccc-en.pdf>.

Based on the CITC's Digital Insights quarterly report for the fourth quarter of 2020, mobile and fixed internet data consumption continues on an upward trajectory, in particular due to the number of smartphone users, increase in data usage during the covid-19 pandemic and the availability of affordable unlimited data packages.<sup>76</sup> We anticipate that the relevant regulators will continue to update and adapt the regulatory landscape to keep up with the market's demands.

## **VII CONCLUSIONS AND OUTLOOK**

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.

Looking ahead, we would not be surprised to see further legislation or regulation in one or more of the following areas:

- a* further development of the national data privacy regime: The PDPL requires the publication of Executive Regulations by the end of the first quarter of 2021, and we expect that these Regulations will add some significant additional detail to the regime created by the PDPL. The PDPL also anticipates that the SDAIA, as the competent authority, may review and update the PDPL directly;
- b* development of specific regulations on the internet of things, autonomous transport, big data and artificial intelligence: As noted above, the CITC has issued some regulations on the internet of things, but we expect the sector will require further regulation as it matures. In addition, the SDAIA has a clear mandate to put in place further regulation, through it and its sub-entities – the NDMO, the NIC and NCAI – to create a data-driven and AI-supported economy in the Kingdom; and
- c* promotion and support for further foreign direct investment in the TMT sector: The Saudi Arabian General Investment Authority was converted into the MISA in 2020 and we expect that throughout 2021 and beyond, the MISA will seek to implement further measures, including potential regulatory reform, to promote Saudi Arabia as a world-class investment destination.

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

---

<sup>76</sup> <https://www.citc.gov.sa/ar/mediacenter/Documents/DigitalInsights-en20q4.pdf>.

## ABOUT THE AUTHORS

### **BRIAN MEENAGH**

*Latham & Watkins LLP*

Brian Meenagh is a partner at Latham & Watkins and leads its Middle East data and technology transactions practice. He represents companies, financial institutions, and government entities in a range of complex transactions involving data, technology and intellectual property assets, both in the Middle East and internationally. Brian serves a diverse client base ranging from startups to governments to many of the world's leading financial services, healthcare and technology companies and has particular experience advising on multi-jurisdictional transactions involving businesses in the Middle East.

### **ALEXANDER HENDRY**

*Latham & Watkins LLP*

Alexander Hendry is a senior associate in Latham & Watkins' data and technology transactions practice. He specialises in the negotiation and drafting of complex technology contracts for commercial transactions and collaborations, and giving strategic advice on large-scale, business-critical, first-of-their-kind technology projects. He advises clients across the globe on legal and commercial issues relating to technology, outsourcing, fintech, commercial contracts, intellectual property, and data privacy. Alexander has practised in the United Kingdom, Asia and the Middle East.

### **HOMAM KHOSHAIM**

*The Law Office of Salman M Al-Sudairi*

Homam Khoshaim is a senior associate in the Law Office of Salman M Al-Sudairi, based in Riyadh. He advises on a broad range of transactions, including M&A, emerging companies, venture capital, joint ventures, initial public offerings and other equity capital markets transactions and corporate advisory work. He also has specialised knowledge in antitrust and competition, payments and emerging financial services, and entertainment, sports and media matters. Homam is qualified in Saudi Arabia, New York and England & Wales (solicitor).

### **LUCY TUCKER**

*Latham & Watkins LLP*

Lucy Tucker is an associate in Latham & Watkins' data and technology transactions practice. Lucy has experience advising clients on a wide range of privacy matters including in relation

to M&A transactions, large scale GDPR transformation projects, regulatory investigations, the privacy risks of new technologies, data processing agreements, international data transfers, direct marketing and the use of cookies. Lucy has also advised on policy and legal matters, including new draft privacy and cybersecurity laws, in the Middle East. Lucy is a certified information privacy technologist (CIPT) and holds a practitioner certificate in data protection.

**AVINASH BALENDRAN**

*Latham & Watkins LLP*

Avinash Balendran is an associate in Latham & Watkins' data and technology transactions practice. Avinash has experience advising clients across a range of sectors including healthcare, private equity, and financial services on a variety of technology and commercial issues. Avinash is also a certified information privacy professional/Europe and has experience advising companies on GDPR compliance projects, on technology-related regulatory issues in the United Arab Emirates and Saudi Arabia, and drafting and negotiating complex commercial contracts through working on a number of landmark deals in the Middle East.

**LATHAM & WATKINS LLP**

ICD Brookfield Place, Level 16  
Dubai International Financial Centre  
PO Box 506698  
Dubai  
United Arab Emirates  
Tel: +971 4 704 6300  
Fax: +971 4 704 6499

**THE LAW OFFICE OF SALMAN M AL-SUDAIRI**

Al-Tatweer Towers, 7th Floor, Tower 1  
King Fahad Highway, PO Box 17411  
Riyadh 11484  
Saudi Arabia  
Tel: +966 11 207 2500  
Fax: +966 11 207 2577

brian.meenagh@lw.com  
alexander.hendry@lw.com  
homam.khoshaim@lw.com  
lucy.tucker@lw.com  
avinash.balendran@lw.com

www.lw.com

an LBR business

ISBN 978-1-83862-834-5