REGIONAL CHANGES IN TELECOMS LAW AND REGULATIONS
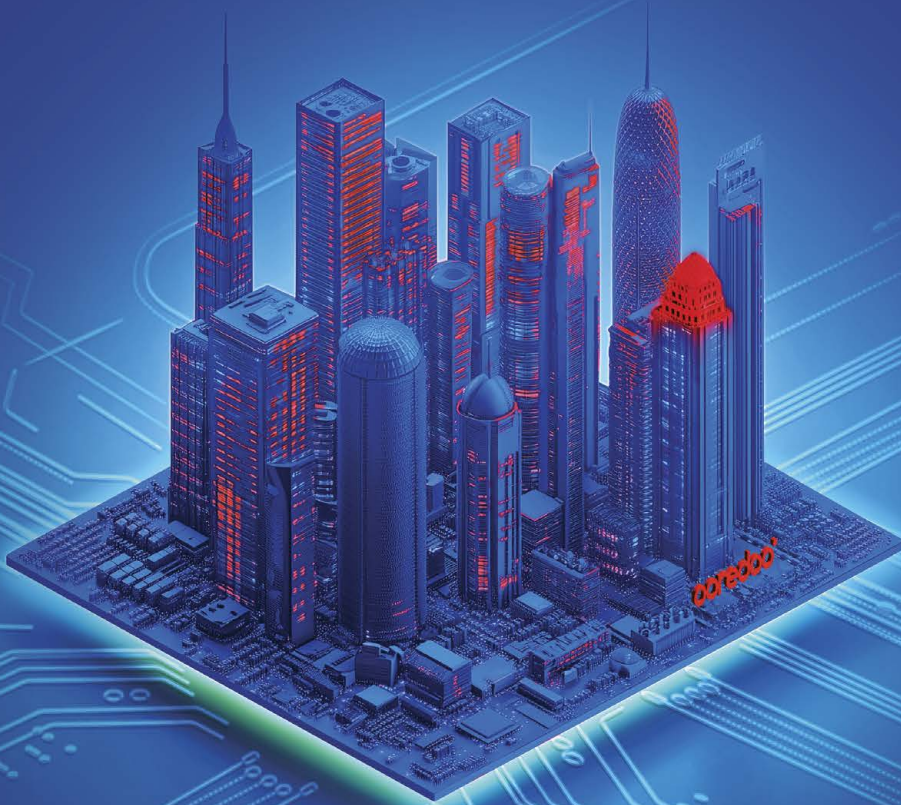
DRIVING A SUCCESSFUL DIGITAL ECONOMY

TECHNOLOGICAL AND LEGAL CHANGE IN THE GCC AND MENA TELECOMS SECTOR

LexisNexis®

ooredoo

YOUR BUSINESS UPGRADED

Providing your business with unparalleled connectivity

UPGRADE YOUR WORLD

ooredoo

LexisNexis

DRIVING DIGITALISATION

In 1983, when the world's first mobile phone became commercially available, the technology landscape was very different from today. The internet had just been 'born' with the development of the Transfer Control Protocol/Internetwork Protocol (TCP/IP), and few could have predicted the range of applications that now fit into the palm of our hands. Telecom services, once a luxury, have become both a ubiquitous and vital part of our daily lives. Now, with the rise of Artificial Intelligence (AI) and Cloud Computing, we find ourselves at another transformative juncture. Governments across the region have recognised the critical role the digital economy can play in driving national development, and companies like Ooredoo are at the heart of these dynamic changes. However, we have also learnt that to unlock the full potential of digital innovation, collaboration is key. Public-private partnerships between regulators, businesses, technology experts, and digital service providers are essential. For such collaboration to succeed, all stakeholders – including legal experts, regulators, and business leaders - must have a deep understanding of the technological opportunities and risks on the horizon. They must also assess whether existing regulations might unnecessarily constrain progress. This special supplement, along with the Ooredoo Group Digital Ecosystem Conference, 'Legislation and Regulation to Drive a Successful Digital Economy' aims to initiate this critical conversation. The conference will examine, through the lens of policy and regulation, the challenges of regulating digital platforms and services, exploring how policymakers can strike the right balance between fostering innovation, investment, and competition while safeguarding consumers and promoting public welfare. In the pages that follow, we will explore topics such as the future of telecoms, AI, cybersecurity, and cloud computing. By doing so, we hope to ensure these innovations have a positive, transformative impact on our lives, just as telecommunications and the internet did back in 1983.

Hilal Al Khulaifi
Group Chief Legal, Regulatory & Governance Officer, Ooredoo Group

Georges Abi Saab
General Counsel, Ooredoo Group

Dr Bharat Vagadia
Executive Director of OG Regulatory Affairs, Ooredoo Group

Mohd Mohannadi
Senior Director, Corporate Governance, Ooredoo Group

Fraser Graham
Director Regulatory Affairs, Ooredoo Group

Haya Al Thani
Senior Analyst - Regulatory, Ooredoo Group

CONTENTS

THE FUTURE OF TELECOMS

Dr Bharat Vagadia of Ooredoo Group explains where the MENA telecoms market is headed from both a technical and regulatory perspective.

"**A** number of the MENA countries have already started to develop national plans to develop their digital ecosystems," Bharat Vagadia states. "Here in Qatar, the Third National Development Strategy 2024-2030 has been looking at how the capabilities of AI and other emerging technology can help drive this forward. The Digital Agenda 2030 which complements the National Development Strategy aims to create 26,000 additional jobs in the Qatari ICT sector by 2030."

"What is important is that the associated changes to the legal and regulatory frameworks which should come with these plans, will also address the regulatory challenges emerging technology can present, as well as continuing to encourage further investments into deploying both mobile and fixed networks."

"The first step on any country's road to digital transformation is having Communication Technology (ICT) infrastructure which provides reliable, affordable connectivity," Vagadia adds. "Connectivity is the bedrock of a digital ecosystem. In the past, this meant connecting phones, then connecting people to the Internet but it is now all about connecting a whole host of devices in a whole range of consumer, industrial and government contexts."

CHANGING APPROACH TO REGULATION

"Good, predictable regulation is critical to digital development," Vagadia explains. "ICT development has policy and regulatory implications across a range of areas, including licensing, spectrum management, standards, competition, security and privacy. The traditional aim of regulation in this sector was to protect broad national interests by focusing on market efficiency and having regulation to ensure industry players' sustainability; to promote competition and efficiency; manage access and use of, sometimes - scarce national resources, such as spectrum; and regulation; and to protects consumer rights and interests."

"Although these regulatory aims are still valid, telecoms regulation can no longer be static," Vagadia adds. "Twenty years ago, when regulators first set out regulations to define the market, things moved gradually. Today in a digital era, innovation drives regulation, not vice versa. Regulation has to respond to industry evolution because policy makers cannot anticipate how and when innovations may change the industry as a result of new emerging technology, business models or services which have become substitutes for existing services."

"When markets and activities within them change in a counterproductive way, regulators need to intervene to redefine the market and/or adopt specific regulations to protect consumers," Vagadia explains. " Non-regulated activities, which create new risks in regulated markets, also need regulatory attention. In this sort of innovation driven environment as the digital economy develops, regulators need to act when non-regulated services threaten either the sustainability of regulated entities through disproportionate competition or to protect consumers. For example, where digital players are offering text, voice and video calling capabilities or satellite operators are providing broadband services without the same regulatory constraints that apply to Mobile Network Operators (MNOs) and that needs to be tackled."

"This may mean regulatory authorities have to converge and/or adjust regulatory powers so they can oversee all elements of bundled end-to-end services and still ensure consistent consumer protection," Vagadia states. "In order to maximise digital benefits, more coordinated regulation across all sectors will be needed. Telecommunications regulators will have to work closely with their counterparts in the data protection and competition authorities, as well as other sectoral regulators in areas including health, agriculture, aviation, and highways. Many others sectors will also have to examine and adapt their

regulations, because of the impact digital technology will have on their markets. This has started to happen in a few countries, such as the UK, Singapore, South Korea and much more work on this is also needed in the MENA region."

"Unfortunately, the haphazard evolution of policies and regulations in the past has led many fixed telecommunications operators to decide that it is more advantageous to separate their businesses into areas still under heavy regulation and those where regulatory constraints might soon be relaxed," Vagadia states. "As a result, globally, many fixed telecommunications operators have sold off their passive infrastructure (which tends to be covered by the most intrusive regulations)."

"Mobile Network Operators (MNOs) are currently looking at whether their tower infrastructure should be carved out," Vagadia adds. "There are also financial reasons for this as tower companies tend to attract higher valuation multiples than integrated operators as investors believe independent tower companies will generate higher tower tenancy rates than telecommunications operators could. As a result, sale and lease back of towers can inject much needed cash into telecommunications businesses. Unfortunately, the MENA legal and regulatory frameworks never contemplated these sorts of market structures so these carve outs can take longer in this region that they would elsewhere."

INVESTING IN INFRASTRUCTURE

"Telecommunications is a capital-intensive business with disappointing returns on investment," Vagadia states. "Establishing the necessary infrastructure to provide nation-wide connectivity, with ever-increasing levels of quality is costly and slow. The technology refresh cycle, especially for mobile operators is now less than 10 years, and these operators need to spend billions of dollars roughly every 10 years. However, consumers who have started to view connectivity as a commodity are becoming less willing to pay the premiums required to support continual investment in their networks for spectrum and equipment."

"5G has required more investment than 4G but most operators found revenues flat lined after 4G investments and revenue uplift after 5G investment is unlikely in the short-term," Vagadia explains. "As a result, many telecoms operators are now exploring new emerging technology, business models and partnerships so they can remain competitive and grow revenue streams."

5G AND IOT

"Consumers (unless they are gamers) may not have noticed a significant change in their network experience, with 5G," Vagadia explains. "However, a main driver for 5G development is the impact it is likely to have on the broader digital ecosystem. Its very design means it is possible to connect millions of devices (Internet of Things (IOT)) on the 5G network, enabling a truly connected ecosystem to develop. Its low latency also means it can be used as a carrier for mission critical applications which traditionally would have needed their own dedicated networks. Therefore, 5G is also a driver for increased use of cloud computing for a broader range of applications and services."

"There are now a whole host of IOT-based products and services," Vagadia states. "Some such as home surveillance video cameras, smart speakers or watches serve consumer needs. IOT is also increasingly being used by businesses and the public sector. IOT has a variety of use cases, e.g. it can be used in agriculture, factories, hospitals, and by government authorities in cities, to provide smart services to citizens. However, only 5% of global IOT revenues come from connectivity components. Around 95% of these revenues are generated by IOT applications, platforms and services or professional services which helps to explain why IOT has been relatively slow to take off and why MNOs have not been pushing IOT as much as they could. It also explains why MNOs are now seeking partners to offer IOT solutions, rather than just IOT connectivity, in order to capture more of the IOT revenue opportunity."

"In order for IOT to really take off an ecosystem of partners; telecoms, software and cloud providers, as well as system and business integrators, needs to come together to develop more effective and scalable solutions to customers' problems."

"This is also an area where a more favourable and predicable regulatory framework is needed," Vagadia states. "Some of the regional regulators have now started to address this. For example, the UAE introduced IOT regulations in 2019, Jordan in 2020 and updated them in 2023. There are now IOT regulations in Egypt, Oman and Bahrain. While, in 2024 Saudi Arabia amended its IOT regulations to simplify some authorisation requirements for IOT provision and enhance IOT security. Qatar have also published guidelines on regulatory requirements to support a forward-looking IOT landscape this year."

FULL FIBRE DEPLOYMENT

"A 5G network is often viewed as a fibre network with antennas which means to get the greatest benefits from a 5G network full nationwide fibre is required," Vagadia explains. "However, this is something which is only available in a few GCC countries. Fibre is considered the most cost-effective way to support 5G networks and increase network capacity for advanced applications such as Augmented Reality (AR), Virtual Reality (VR), and in the future Metaverse. However, it requires significant upfront investment (mainly for engineering work like digging up roads to lay ducts or fibres into the ground). Therefore, as data traffic grows, policy makers are urging operators and governments to prioritise investment in full fibre broadband networks. It is seen by many as 'future-proof' infrastructure. Although civil engineering costs of initial deployment are high, once deployed, increasing network capacity of full-fibre networks is relatively cheap, as no changes to network architecture are needed, just equipment upgrades."

Dr Bharat Vagadia

Executive Director of OG Regulatory, Ooredoo Group

"However, with payback periods over a decade for the initial infrastructure it has been difficult for many MNOs to invest the required capital," Vagadia continues. "Therefore, this will be another area Governments in the region will need to effectively address. At present there has been a lack of widespread fibre deployment and no real killer applications for 5G, so most 5G deployments have been carried out gradually, as an evolution of 4G networks using 5G Non-Standalone technology (NSA). The strategy has been to gradually migrate to the 5G Standalone technology (SA) when the market conditions are appropriate or as may be mandated by the licence, which slows the process."

5G PRIVATE NETWORKS

"However, one way of potentially monetising 5G network investment is by deploying 5G private networks," Vagadia explains. "Private wireless networks are not new, and have been deployed on LTE spectrum (4G) for several years but 5G's arrival has given new

impetus to private network interest and has led to more solution providers directly engaging with enterprises. With 5G's performance advantages over 4G and WiFi and advances in related technologies, such as Edge Computing, private 5G network numbers are expected to rise rapidly in the future. Initial deployments have tended to focus on large scale industrial applications. In the MENA region, we are now seeing ports, oil and gas companies, hospitals and some large-scale factories looking at private 5G networks as a way to connect their infrastructure. This allows them to quickly reconfigure their environments to meet changing demand or even changes in business models, with the assurances of reliability that 5G offers."

"In most of the regional markets these private 5G networks are still provided by the traditional licensed mobile operators, but in other parts of the world, e.g. USA, Asia and Europe, separate private networks are being established by the entities themselves, and in some parts of the world, regulators have been considering setting aside spectrum for separate private networks created by enterprises, which is creating a greater disparity in regulatory treatment between traditional MNOs and new players."

RETIRING 3G

"Another change as a result of the 5G launch is that older technology is being retired, as 3G use declines and consumers move to 4G and 5G," Vagadia states. "In Jordan and Bahrain MNOs voluntarily switched off their 2G networks in 2021. Saudia Arabia and UAE mandated 3G switched off in 2022, and Kuwait a year later. Oman has mandated switch off this year and Qatar is reviewing its switch off dates. Algeria, Tunisia and Morocco which have technology specific licences may wait for the 2G and 3G licences to expire before their switch offs."

DIGITAL SERVICE

"Another obvious trend in the MENA region has been the growth of digital services, including e-commerce, marketplaces, fintech and streaming entertainment services," Vagadia states. "This has led to greater investment in data centres and international connectivity through submarine cables. Ooredoo Group have separated out its data centres into a separate business (MENA Digital Hub) and have partnered with NVIDIA to leverage their cutting-edge accelerated computing platform."

NET NEUTRALITY SERVICE

"On a less positive note, a worrying policy development in the region has been the introduction of net neutrality, as countries including Qatar and Saudi Arabia, follow an approach taken in Europe," Vagadia explains. "This is the concept that internet service providers should enable access to all content and applications, without favouring or blocking particular websites or products. It is being seen as a negative development for MNOs

who have already been making poor returns on capital. While digital players like Apple, Microsoft, Google, Meta, , TikTok, Amazon, and Netflix have benefited from this approach, net neutrality regulation, means MNOs are unable to incentivise those digital players to limit the data they produce, e.g. by compressing videos, or stopping auto-run video play which is pushing greater data levels down MNOs' networks requiring them to invest growing amounts in expanding network capacity, with little financial benefit from doing so."

SATELLITE DIRECT TO DEVICE (D2D)

"Another interesting development is Satellite Direct to Device (D2D)," Vagadia continues. "Non-Terrestrial Networks (NTNs) have been used in the past by mobile operators to extend network coverage through Geostationary Equatorial Orbit (GEO) satellite backhaul. Although, the high costs of these solutions mean they were only used for a tiny amount of connectivity."

"However, advances in technology, and greater investment in satellites have now created a flurry of activity in the area," Vagadia explains. "We are now seeing low-earth orbit (LEO) satellites, High-Altitude Platform Systems (HAPS), as well as D2D LEO satellites emerging. The business model for some of these is to work with MNOs to extend their coverage, especially in rural areas. For others the model involves supplying broadband services directly to consumers, through new terminals, or consumers' existing mobile devices."

"There are a number of players in this space including Amazon Kuiper, SpaceX Starlink, OneWeb, AST SpaceMobile and LynkGlobal," Vagadia states. "With the expansion of new types of non-terrestrial infrastructure and new services (e.g. broadband with relatively higher speeds and lower latency than traditional satellite systems), these services and mobile network-based services are becoming more similar. However, currently regulators are treating these additional offerings by satellite network providers in a different way to how they regulate traditional MNO offerings."

"These mega constellation-based satellite providers tend to benefit from existing satellite regulations which were originally designed to tackle the provision of limited, traditional satellite services, and has led to a lack of regulatory parity between these increasingly converging services," Vagadia adds. "As a result, there are concerns with these new services, as well as a whole host of regulatory gaps on areas including minimum service quality levels, and infrastructure sharing. There are also gaps on fiscal areas such as the universal service fund levy, mobile-specific taxes and fees."

"Most regulation, especially spectrum regulation, is multi-national," Vagadia explains. "There are bodies which handle regional and global regulation, including the International Telecommunications Union (ITU). However, the need for regulation and its character has changed dramatically. Multinational regulation in this area has

not kept up. For example, there is highly dysfunctional behaviour in satellite allocation as some large LEO operators file for thousands of satellites through countries like Rwanda and others broadly ignore the filing process, instead operating under 'opt-out' clauses. World Radiocommunication Conferences (WRC) meetings every four years are unable to handle an urgent need to tackle how direct-to-device satellite allocations might work, especially when they reuse terrestrial spectrum. New ways of resolving this issue, either within or alongside the ITU and regional bodies are needed."

ENABLING DIGITALISATION THROUGH APIS

"Given the previous difficulties MNOs have had in capturing the growth of the digital economy, another exciting development has been the move to open Application Protocol Interfaces (APIs), which may help facilitate additional ways MNOs can work with digital players in a partnership model," Vagadia states. "Many MNOs are considering opening up their networks so they are more closely integrated with these players through the use of APIs. Some view this as an MNO move towards a platform play, trying to mimic business and operating models of the digital players but by opening up their APIs, MNOs are enabling third-party developers to create innovative applications and services which integrate seamlessly with their networks, while also being able to charge transaction fees each time these networks, assets or their intelligence is provided to these third parties, or vice-versa. For example, by integrating location-based services from MNOs with mapping services from technology companies, enhanced navigation and tracking solutions are possible. This integration also enables customers to have a more personalised, contextual experience, enabling MNOs to offer bundled services, cross-promotions, and tailored recommendations. However, the biggest sticking point in opening access to network APIs and capabilities may be security concerns that have held telecoms back from embracing APIs fully. For example, in 2023, US operator T-Mobile suffered a security breach via an unprotected API which compromised the data of 37 million customers."

ARTIFICIAL INTELLIGENCE

"There have also been some significant technical and regulatory developments on AI in the region," Vagadia states. "For example, in September 2024, the Qatar Central Bank (QCB) issued AI guidelines which apply to any entity the Qatari Central Bank licences. Other significant developments in Qatar have included the development of an indigenous Large Language Model (Al Fanar), a tripling of data centre capacity, and the procurement of high-performance computing resources (Nvidia). AI is now at the heart of many applications but with its potential comes vital questions which will determine its future success, and how it impacts society. As AI needs vast amounts of data to feed its ability to learn and adapt, firms with access

to data will become key players in the AI economy, potentially at the expense of others and ultimately also consumers," Vagadia continues. "To generate the required data to drive these AI algorithms, use of more intrusive means of acquiring personal data and associated meta data could become more common striking at the heart of personal privacy. As AI advances, its use cases will mushroom, some applications will deliver much needed solutions in sectors such as healthcare, but others could potentially be used by unscrupulous people."

"Countries are currently taking different approaches to AI regulation, and in some cases those approaches are changing," Vagadia states. "China has been using a principles-based approach, as have the UK and the USA but there are ongoing discussions to strengthen these requirements. The EU has taken a risk based approach with legislation to regulate some AI applications that pose risk of harm and it is likely the extra-territorial jurisdiction of the EU AI Act will impact global AI development and deployment. In the absence of firm AI regulations, many organisations that use or embed AI into their processes or products have also developed their own AI ethics which tend to follow the OECD principles for trustworthy AI - fairness, transparency and explainability, accountability, safety and robustness, human agency and oversight, privacy and security and in some cases environmental impact. Across the GCC, Qatar has developed an AI policy which identifies six pillars - education, data access, employment, business, research, and ethics, which will guide the state towards an AI future. In 2017 the UAE government established an AI Ministry called the Artificial Intelligence, Digital Economy and Remote Work Applications Office which is part of the UAE Council for Artificial Intelligence and Blockchain. The UAE's AI Ethics Principles now provide a foundational ethical framework for AI development and deployment there."

"In Saudi Arabia, a National Strategy has been developed by the Saudi Data and Artificial Intelligence Authority (SDAIA) whose AI Ethics Principles is the first AI regulatory framework there," states Vagadia. "In April 2024, Bahrain also issued a new law on AI and has a set of principles and values guiding the ethical use of AI. A consultation on AI policy has been issued by the Omani Ministry of Transport, Communications, and Information Technology (MTCIT), suggesting that, since the final document will not be mandatory, MTCIT does not intend to impose significant restrictions on the use of AI systems in Oman. This indicates a preference for fostering an open environment that encourages AI innovation, rather than stifling it with rigid rules. However, what will be crucial, both in Oman and in other jurisdictions, is that the laws and regulations established are fair and provide necessary protections. At the same time, regulators must remain agile enough to adapt to emerging innovations that have yet to be conceived as they evolve, ensuring a balanced approach between fostering technological growth and safeguarding public interests."

NEWS ROUND-UP
COVERING LEGAL AND REGULATORY CHANGE REGION-WIDE

AI AGREEMENT WITH UK

The Qatar Research, Development and Innovation Council has invited non-profit, non-governmental organisations and government entities from around the world with expertise in AI and related fields to submit proposals which will help support the development of the artificial intelligence strategy in Qatar and the UK, as part of an agreement between the two countries. It is hoped the initiative will provide new opportunities to Qatari graduates and help with a review of the potential opportunities for increased cooperation between the two countries on the launch of AI based companies.

NDS3 AND PLANS FOR THE DIGITAL ECONOMY

As part of its Qatar National Vision 2030 (QNV 2030), Qatar has launched its third National Development Strategy (NDS-3). This aims to strengthen both physical and digital infrastructure in the country. Qatar views Public Private Partnerships (PPPs) as a key strategy which will be used to meet these infrastructure development goals, and the Qatar PPP market is expected to grow in the coming years providing significant opportunities for local and international investors, across various sectors. A key element in the plan is the construction of Smart Cities such as Msheireb and Lusail which have been specifically designed to optimise sustainability and minimise emissions. In addition, as Qatar's economy transitions to a knowledge based one, the focus will be on enhancing the local and expatriate community in Qatar's skills in areas such as digitisation, AI and sustainability.

CENTRAL BANK ISSUES AI GUIDELINES

The Qatar Central Bank (QCB) has issued Artificial Intelligence (AI) Guidelines which will regulate the use of AI in the financial sector. The Central Bank has stated adopting AI technology offers various benefits to financial institutions. They are allowing them to explore its potential to develop products and services for customers. The Central Bank is keen for financial institutions in Qatar to keep pace with the latest international practices and standards. It also recognises the role AI can have in helping the financial sector to reduce costs, improve operational efficiency and speed up service delivery. A key driver for Qatar's national digital transformation is Digital Agenda 2030 (DA 2030) which aims to accelerate growth and transform Qatar into a globally competitive, diversified and innovative digital economy. Cross-border digital exchange including cross border data flows and digital inclusion have been identified as supporting factors for achieving this.

DIGITAL ASSETS LAW

The DIFC has issued a ground-breaking law DIFC Law No. 2/2024 the Digital Assets Law. The law sets out the legal characteristics of digital assets for the purposes of property law, and specifies how digital assets can be controlled, transferred and dealt with by parties. Digital Assets are a growing asset class with scope for future innovation, particularly in asset tokenisation. However, to date there had been a lack of certainty on their precise legal nature. A new tort of impairment has also been introduced in this law. The changes brought in by DIFC Law No. 2/2024 have also had a wide ranging impact on a whole host of other laws as a result. Therefore, as a result of this law, an amending law DIFC Law No. 3/2024 has also had to be issued which has brought in changes to DIFC law on areas including contracts, trusts, foundations, insolvency, and implied and unfair terms in contracts . There have also been changes to DIFC law on obligations and damages, and remedies. A new DIFC Security Law DIFC Law No. 4/2024 has also been issued, partly as a result of DIFC Law No. 2/2024. To make it easier to understand the Digital Assets Law's impact on these other laws, the DIFC has for the first time included a special schedule, Schedule 2 of DIFC No. 2/2024 which explains the relevant changes to each of these laws.

STANDARD DATA PROTECTION CLAUSES

The DIFC has issued standard data protection contractual clauses which can be used where a DIFC Exporter wishes to transfer data to a Non-DIFC Importer in a third country which has either no or unrecognised data protection laws. The clauses have been drafted in line with Article 26 and 27 of DIFC Law No. 5/2020 (which is the DIFC Data Protection Law). Areas covered include onward transfers, what should happen where sub-processors are used and what would happen if local laws and practices might affect compliance with the clauses. There is also an optional docking clause which covers when an entity that is not a Party to these Clauses, with the agreement of the Parties, accedes to the Clauses.

AI AND WELLBEING

The UAE Government has issued a Charter those wishing to develop or adopt artificial intelligence there, should review. The charter supports the UAE's AI strategy for 2031 which aims to transform the UAE into a pioneer in AI by investing in people and industries. The charter's main aim is to enhance the safety and privacy standards which are followed when AI technology is created and applied. UAE authorities are keen to ensure AI developers and users put human values and rights at the heart of technological innovations. It sets out 12 general principles, which focus on strengthening human and machine relationships in ways that support human wellbeing and progress. Importance is placed on safety, fairness, privacy and transparency. It also includes principles which are designed to boost governance and accountability in AI to ensure the technology is used ethically

and transparently, and emphasises the importance of compliance with international treaties and local laws on the development and use of AI.

GUIDANCE ON DATA PROTECTION

In order to support those looking to comply with the implementation of the Saudi Arabia Data Protection Law (Saudi Arabia Cabinet Decision No. 98/1443) and its relevant implementing regulations (Saudi Arabia Administrative Decision No. 1516/1445 Approving the Implementing Regulation of the Personal Data Protection Law) from 14 September 2024 a host of new guidelines have been issued by the Saudi Data and Artificial Intelligence Authority (SDAIA). These include the Personal Data Disclosure Cases Guideline which outlines six cases where data may legally be disclosed under the law. The Minimum Personal Data Determination Guideline also provides a framework to help entities ensure only the minimum necessary personal data is collected for any specific purpose. There is also the Elaboration and Developing Privacy Policy Guideline which helps those creating privacy policies. In addition, rules for appointing a Personal Data Protection Officer (DPO) have been issued as have regulations on data transfers outside Saudi. Finally, there is a Binding Common Rules Guideline which is designed to assist with personal data protection for international transfers within multinational groups.

THE SAFE USE OF GENERATIVE AI

Saudi Arabia's Data and Artificial Intelligence Authority (SDAIA). has issued guidelines on the safe use of Generative Artificial Intelligence. The guidelines cover government data usage as it relates to integrity, fairness, reliability, safety, transparency, interpretability, accountability, responsibility, privacy, security and social and environmental benefits. These guidelines complement existing rules and regulations on areas including AI ethics, data governance, privacy, security, intellectual property and human rights.

DATA PROTECTION REGULATIONS

New Data Privacy Regulations Kuwait Administrative Decision No. 26/2024 have been issued in Kuwait which have repealed and replaced Kuwait's previous data protection regulations (Kuwait Decision No. 42/2021) which were issued back in 2021. The Regulations cover a number of issues including the conditions for collecting and processing persona data. They also explain the conditions which must apply in order for any collection and processing of this data to be deemed to be legal. In addition, there are detailed requirements on the steps service providers must take to ensure personal data is secure and protected and the way in which the authorities must be notified when there is a personal data breach. Where the regulations are breached and there has been a violation of these provisions the Kuwait Communication and Information Technology Regulatory Authority has the power to apply penalties and fines listed in Kuwait Law No. 37/2014 On the Establishment of the Telecommunications and Information Technology Regulatory Authority.

TELECOMMUNICATION DEVICES

The Oman Telecommunications Regulatory Authority has issued Decision No. 1152/2/19/2024 on regulations on Organisation and Approval of Telecommunication Devices. This decision repeals and replaces Oman Decision No. 59/2015 which regulated communications devices. The Decision prohibits trade in telecommunications devices, such as radio and terminal telecommunications devices in Oman unless that type of device has been approved by the authority, although the Chief Executive Officer can issue decisions granting exceptions. In addition, it is forbidden to import telecommunications devices into Oman without first having a permit to do so from the Authority. Local manufacturers of devices of this type

REGULATORY ROUND-UP

Qatar: The Qatari Central Bank has issued Digital Insurer Regulations which define the regulatory framework for digital insurer activities there…

GCC: Following an agreement between the GCC and Bahrain and the issue of Bahrain Law No. 3/2024 the Technical Telecommunications Office has been established in Bahrain…

Oman: Oman Telecommunications Regulatory Authority Decision No. 1152/2/10/2023-20 on the issuance of the access and interconnection regulation which involves the technical, regulatory and financial standards that allow two or more public telecommunications networks in Oman to be connected to each other to transfer telecommunications traffic from one network to another has been issued…

UAE: The UAE Central Bank has issued Circular No. 2/2024 which sets out a comprehensive framework for licensing and supervising digital payment services…

Qatar: Qatar's Cabinet has approved a draft Prime Ministerial Decision proposing the establishment of a Digital Government Steering Committee…

DIFC: The DIFC Courts have issued guidelines on the use of AI generated content in court proceedings…

Oman: Oman's Telecommunications Regulatory Authority has confirmed that only companies licensed by the Authority can deliver e-commerce products…

Dubai: The Dubai Cyber Security Centre has launched a list of accredited cyber service providers as part of the Dubai Cyber Security Shield initiative…

UAE The Dubai Securities and Commodities Authority (SCA) has issued guidelines on the regulations on virtual assets and virtual asset service providers…

must also submit an application to the Telecommunications Regulatory Authority after these devices have been manufactured and before they are either used, sold or displayed. Approvals are also needed before storing, selling, receiving, delivering, exporting or destroying radio telecommunications devices that require radio licences. In addition, telecommunications devices which are approved by the Authority will also need to have an accreditation label on them.

CONSUMERS: THE RIGHT APPROACH

Ken Wong and Ben Gibson of CMS explain the way in which consumer protection is dealt with in the telecoms sector in Saudi Arabia and the UAE.

"The telecommunications markets in Saudi Arabia and the UAE are quite different," states Ken Wong. "The UAE market is a duopoly with two main operators, Etisalat and du. Licensing is strict, and international providers must partner with local operators to offer services. In contrast the market in Saudi is more open. There are a number of operators there, including STC, Mobily, and Zain. Licensing is also stringent, but there is more competition. However, one common feature of both these telecoms markets is the robust approach to customer protection."

ADVERTISING AND SALES

"In Saudi Arabia, the telecommunications sector is regulated by the Communications, Space and Technology Commission (CST)," Wong explains. "In 2020 they issued the Regulations on the Protection of Rights of ICT Services' Users and on the Terms of ICT Service Provision. Under Article 3(1) of these regulations at all times service providers must provide across all their sales outlets, on their website, or on any other channels they use clear, up-to-date and full information on their retail tariffs. These also have to be fully consistent with the tariffs offered in user service contracts and those they have provided to the CST."

"Transparency and clarity of information advertised via all promotional or advertising channels on any packages or service offers are required," Wong adds. "In addition, if there are any restrictions, or terms of use, or obligations, they should also be mentioned in the advertisement, in a way that does not mislead users. Service providers also have to use their own approved trademarks in these communications."

"Article 4 of the regulations covers the telemarketing of telecoms services," Wong adds. "These rules are also quite strict. For example, service providers cannot telemarket their services or products for sales purposes to users without the user's prior consent. In addition, they can only

contact the user through the service provider's official communication channels. Users can also block telemarketing free of charge."

"In the UAE, the Telecommunications and Digital Government Regulatory Authority (TDRA) regulates the telecoms market," states Ben Gibson. "They have issued Consumer Protection Regulations which cover areas including fair treatment of consumers, billing transparency, and the availability of complaint mechanisms. There are also Service Transparency Regulations requiring telecoms companies to provide detailed information on their services, including coverage areas, service quality, and any limitations. In addition, the TDRA has issued a specific Internet of Things (IoT) Policy which sets out the registration, compliance, security measure, and transparency requirements of IoT services in the UAE."

"New regulations have also been issued with specific requirements on telemarketing in Cabinet Decision No. 56/2024 and Cabinet Decision No. 57/2024. These apply to any sector, including when selling telecoms products and services. There is also a sector neutral consumer law and implementing regulations (Federal Law No. 15/2020 and Cabinet Decision No. 66/2023) which cover areas including advertising, labelling, pricing and e-commerce restrictions, those in the telecoms sector must consider."

TELECOMS CONTRACTS

"However, it is not merely advertising and sales, where detailed requirements impact the telecoms sector," Wong states. "There is also a long list of information which has to be provided to customers in telecoms contracts in these jurisdictions."

"In Saudi Arabia, telecoms contracts must include details of the tariffs and charges for the services, equipment and devices provided, which distinguish periodic and any non-periodic charges, whether at the start or the end of the service. There must also be details of all the services, products and their features which the service provider must provide, as well as the means of agreeing a settlement if there is a failure to meet any of the quality parameters approved by the CST or stipulated in the contract."

"One particularly interesting requirement is that anyone agreeing a telecoms contract in Saudi must be at least 15 Hijri years and an application for establishing a service may not be accepted if it is made in the name of someone who is under that age, even if their legal representative is over that age," Wong explains. "Telecoms contracts also need to be either in Arabic and English, in clear, legible language which is easy to understand. The user's consent to the contract is needed and if there is a dispute the service provider would have to prove the user's consent to the relevant contract terms and conditions. Service providers also have to provide users with a copy of the service contract once completed and need to retain the contract in line with required time limits."

"In the UAE details of the required provisions in telecoms contracts are currently found in TDRA Consumer Protection Regulations (Version 2.0)," states Gibson. "These regulations require telecoms providers to clearly outline in their contracts, areas including pricing, duration, and penalties for early termination. Telecoms providers also have to ensure that subscriber contracts are transparent, and that subscribers receive a contract which details the full terms and conditions. These terms which are detailed in the Consumer Protection Regulations are seen as a minimum and the TDRA can require a Licensee to amend their Subscriber contracts if they do not comply with their regulatory framework."

"The TDRA requires telecoms providers to notify consumers of any price increases at least 28 days before any price increases or contractual changes which affect pricing," Gibson adds. "Consumers also have the right to terminate the contract without any penalty before such price changes take effect."

BILLING

"Another area where there are specific consumer rights is on billings," Wong adds. "In Saudi Arabia, Article 15 of the Regulations on the Protection of Rights of ICT Services' Users and on the Terms of ICT Service Provision covers this. Services providers have to provide consumers with a free and easy means to monitor the consumption of services they have used. There are also specific requirements on postpaid customer billing. For example, invoices must be issued at the end of every calendar month and cannot be invoiced for any service charges in advance for postpaid services or claim any other charges until after the end of the billing cycle."

"Service providers must provide users with clear, correct and detailed invoices in Arabic and English, depending on user choice, and send them electronically, free of charge. Users must also be able to access online a system which enables them to obtain copies of their pending or earlier detailed invoices, for a minimum of 12 months from the date of invoice issue. It must also be possible for users to save or print these invoices."

"In addition, as well as the usual sorts of information that might be expected in telecoms invoices, in Saudi they must include the termination date for non-payment and suspension date, details of any non-periodic charges, settlement and deposit amounts, loyalty programme details, and an express reference to the user's right to review the invoice and object to the charges stated in it within 60 days from its issue."

"In the UAE, Article 3.9 of TDRA Consumer Protection Regulations (Version 2.0) states subscriber invoices and billing data must be retained for at least two years," Gibson explains. " Written contracts for new subscribers must also clearly state billing timeframes, cycles, and payment methods. In addition, Article 27.1 of the TDRA Consumer Protection Regulations (Version 2.0) requires telecoms providers to audit their billing systems and submit signed audit reports to the TDRA at intervals specified by the Authority."

Ken Wong
Partner, CMS

Ben Gibson
Partner, CMS

SERVICE QUALITY

"In the UAE the TDRA has issued a Quality of Service (QoS) Policy which sets standards on the quality of telecommunications services, including network performance, reliability, and customer service," states Gibson. "In addition, Article 13 of Federal Law No. 3/2003 (the Telecommunications Sector Law) states telecom providers must provide services in a manner that meets the standards of good performance set by the regulatory authority, ensuring the services are adequate and reliable. The UAE Consumer Protection Law (Federal Law No. 15/2020) also provides consumers with the right to a standard quality of goods and services."

"In Saudi Article 13 of the Regulations on the Protection of Rights of ICT Services' Users and on the Terms of ICT Service Provision requires service providers to promptly address any service failures or interruptions," Wong states.

"This includes rectifying issues as soon as they are identified by the service provider or reported by a user. A key point to note is that during service disruptions, the service provider cannot impose any additional charges on users."

"There are a number of specific requirements on carrying out repairs. Service providers are responsible for the proper functioning and timely repair of network components beyond the user's premises, which includes any devices or equipment installed or provided by the service provider within the user's premises."

"Finally, there is a provision those who report a fault are likely to appreciate. When faults are reported, a text must be sent providing details including how long the fault might take to repair, the date and time of the visit, any compensation details, as well as a fix notification."

RELATED LEGISLATION

Article 3(1) of Cabinet Decision No. 56/2024
When marketing products or services through phone calls, companies shall commit to paying due care and adequate attention to everything that would prevent consumer inconvenience and adhering to the highest standards of transparency, credibility and integrity.

(Source: Lexis Middle East Law)

QICDRC Legal Clinic

Specialised Panel Law Firms offering complimentary consultations for civil and commercial cases

العيادة القانونية لمحكمة قطر الدولية

تقديم المساعدة القانونية في المسائل المدنية والتجارية من خلال مكاتب محاماة معتمدة

ARTIFICIAL INTELLIGENCE

Umar Azmeh, Registrar at the Qatar International Court and Dispute Resolution Centre (QICDRC) explains how AI is helping the GCC legal profession and courts to become smarter and more efficient, but also where the risks and future benefits might be.

"With the public release of scaled large language models (LLMs) such as ChatGPT, industries and sectors of all types across the world have been looking at ways in which they can harness and benefit from Artificial Intelligence (AI)," states Umar Azmeh, Registrar at the Qatar International Court and Dispute Resolution Centre (QICDRC). "In this respect, Middle East Courts, including the QICDRC in Qatar are no different."

POTENTIAL USES

"Within a court system, an AI system can either be internal facing or external facing," Azmeh continues. "Internal AI systems can assist the court, court staff and judges with case progression and decision-making. For example, AI can be used to scan and review case papers which are often long, made up of huge numbers of documents and can include complex data, in order, say to provide summaries of complex financial data which identifies patterns, or they can be used to automate procedural tasks such as the acceptance and service of a case on behalf of a claimant, which helps make judicial procedures faster and cheaper, improving access to justice."

"In contrast, external facing AI in a court context is technology which assists court users," Azmeh continues. "For example, it may be possible to put programs in place that review the paperwork which has to be provided to the court to ensure the parties have fulfilled all the mandatory requirements when they file their case and reduce the risk of cases being rejected because of purely procedural mistakes."

"Since our first case in 2009, the QICDRC Courts have prided themselves with having a case management system that has a strong technological setup through which cases process, and having an online hearing system which allows simultaneous translation so parties from all over the world can participate in cases being heard in our courts live on our website," Azmeh adds. "However, we have also been keen to learn more about the ways some other courts are now using AI both externally and internally."

"Last year we visited courts in Shanghai and Hong Kong, in particular the Shanghai Financial Court and the High Court of Hong Kong, to learn more about the AI technology they have begun using," Azmeh states. "Of particular interest to us at the QICDRC was the simultaneous translation and transcription software the courts in Shanghai had developed. As a dual language (English and Arabic) court being able to simultaneously translate and transcribe either English to Arabic, or vice versa (as well as potentially extending the application to other languages since we have parties from all over the world) is a key potential development."

"Using AI in this way in our court would ensure accurate transcripts were instantaneously available," Azmeh continues. "It would also reduce our reliance on translators and lead to significant savings."

"We were also very interested in the way, AI was being used in the courts in Shanghai and Hong Kong to enable 'smart presentation'," Azmeh states. "A sophisticated, integrated system is being used there, linked to all the screens in the court room, which enables parties to call up evidence from large bundles. The parties and their lawyers can then either privately mark up those documents on their own screen or quickly compare one document to others in the case files. These types of application can, particularly in paper-heavy cases, make trial processes much smoother and more efficient."

"Another impressive program being used by the courts in Shanghai scanned all the case papers filed and served by the parties and converted them into a particular format which was also readable," Azmeh continues. "This allows the court to quickly check, for example, pleadings the parties have made are complete and legally sound before the case has moved on to its next phase."

"Parties involved in litigation can often make small mistakes which slow the litigation process down, add to costs or which can even lead to cases being dismissed," Azmeh adds. "Therefore, using AI this way helps ensure the court functions as efficiently as possible and reduces litigation costs for parties. These sorts of applications enable courts to save time and resources. They also help to ensure cases are dealt with as efficiently as possible because the claims submitted are complete, which improves a court user's experience."

"However, it is not just once cases are filed where AI is benefiting parties in disputes," Azmeh continues. "AI is also now being used in the legal profession to make savings at an earlier stage. For example, it is being used for what is called outcome prediction. There are now applications lawyers can use to analyse the documents which would be filed with the courts, before that happens and then predict the case outcome based on various factors. These include legal factors such as the type of evidence available, the nature of the claim and the remedy being sought, but also precedents (i.e. what has been decided in similar cases in the past) and so called extra legal factors (which might include the general approach taken by a particular court or even judge). With this information, the parties and their lawyers can potentially assess the risks they will not be successful and may avoid incurring unnecessary court costs on cases they are unlikely to win."

POTENTIAL RISKS

"However, the use of AI in courts for litigation purposes or in the course of litigation can also raise a number of legal, ethical and moral issues," Azmeh states.

"For example, there was what has become an infamous US case where a lawyer used AI to assist him in drafting a legal document and the purported precedent deployed in court which was generated using an AI program was later found to be fictitious. Thankfully in this case, the error was discovered before the court made an erroneous decision based upon it."
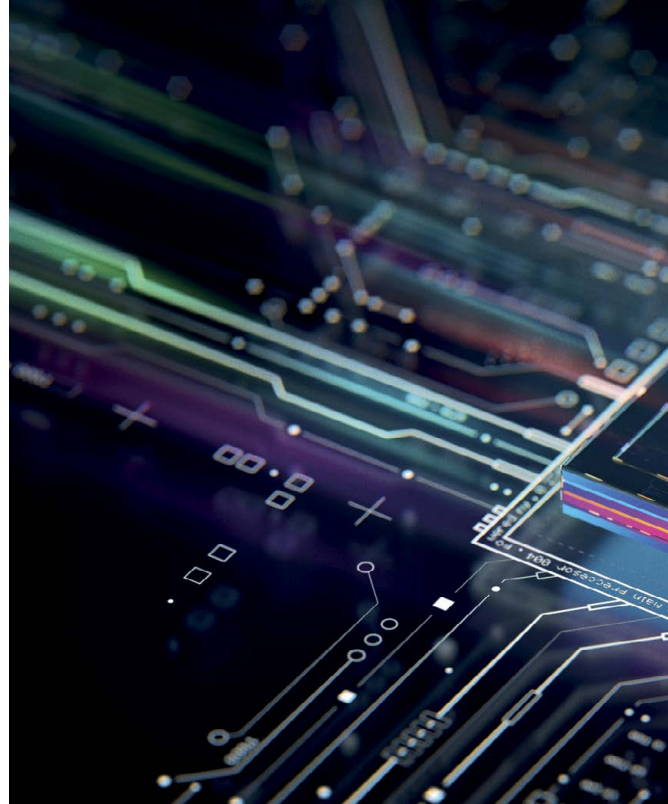
"As a result, I believe it is important for courts to make it clear to lawyers what their disclosure obligations are in such cases," Azmeh adds. "This is, particularly important in a court like ours where lawyers from very many different jurisdictions appear, all of whom will have their own regulatory and ethical obligations in their home jurisdictions."

"When it comes to the use of AI in court proceedings, transparency and consent are very important. This means clearly disclosing not just that AI has been used but what the source of the AI-generated content is, and any potential limitations or biases associated with the AI system."

"One issue GCC courts have been recently considering is when the use or even potential use of AI in the case process should be disclosed to the other party," Azmeh adds.

"This is important as if parties wait till shortly before the case is about to start or during the trial itself to disclose this there could be a risk of their opponent requesting an adjournment. The court may feel it is necessary to issue case management orders specifying how AI content can be used in the proceedings. Some courts may also require the consent of the other party before AI generative content can be used in a case."

"Reliability and accuracy are also very important when AI generated data is used by lawyers in Court," Azmeh explains.

"Parties should avoid being overly reliant on LLMs or generative content generators (GCGs) which produce content of a particular type to produce documents for legal proceedings," Azmeh states. "AI technology can be very useful in assisting lawyers when putting forward submissions for their legal proceedings but it is also important to consider the risks – what algorithms and training data has been used and what is the potential for bias or inaccuracy. Human decision making still needs to be part of the process when preparing evidence or submissions for court."
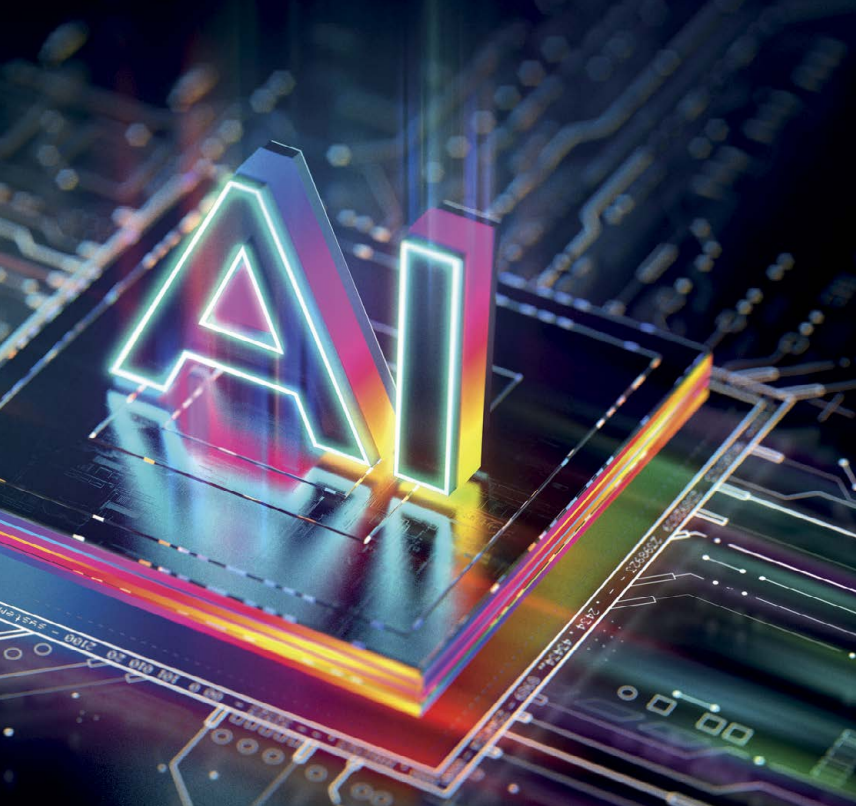
considerations apply when developing and rolling out any new technology, including new AI systems. Therefore, where AI is using personal data or might risk privacy it is important to follow best practice and ensure data protection legislation will be complied with whenever new technology is being considered."

INTELLECTUAL PROPERTY

"Another area where AI use may increase legal risk is intellectual property," Azmeh states. "AI models trained on copyrighted data, such as books, images, and articles, can potentially produce content that infringes copyright if they produce content which is similar to copyrighted materials. There can also be risks when confidential data is input into AI models, as it could learn or expose trade secrets. However, in the future, AI may also be able to assist clients and lawyers to better understand the contours of a complex area like patents to ensure that they are not breaching intellectual property rights."

WHAT'S NEXT

"Legislators and regulators in Qatar have recently been working on new legislation and regulations to support the digital economy in Qatar," Azmeh states. "For example, the QFC's Digital Asset Regulations include definitions of a range of technical terms including tokens, and cover their ownership, transfer and control, as well as regulating the provision of token services for QFC entities and detailing the penalties for breaches."

"In addition, the Qatar Central Bank has recently announced the launch of its digital currency project which aims to leverage AI technology, distributed ledger technology and emerging technology in order to establish 'a strong foundation to enhance liquidity by expanding participation in financial market facilities'. So there is currently a large amount of work being done in Qatar on AI and related issues, and more legislation and regulation on a whole host of areas is expected."

"Over the next five to ten years, I expect there will be significant and positive changes in the legal sector in the GCC as a result of greater use and innovation using AI," Azmeh continues. "Within the courts, the main opportunities in my opinion will come from the significant savings in time and resources, which will be important as generally courts are public bodies with finite resources. In addition, the AI innovations we are already starting to see will make case management processes easier and more efficient – resulting in greater access to justices. There is also the potential for a greater use of AI decision making tools by lawyers at the pre-litigation stage but also potentially in the future by judges. There I would expect AI tools will be used as decision making aids by judges, rather than a means of making automatic final decisions in cases. AI has the potential to become a very valuable tool for judges in the courts, as it could sift through large volumes of material to spot patterns judges could then interpret, improving the consistency of case decisions."

DATA PROTECTION AND PRIVACY

"However, the potential issues when parties and lawyers wish to use AI generated content in courts are not just technical ones," Azmeh states. "There can also be additional legal risks, including on data protection and confidentiality. AI systems tend to process and analyse huge amounts of data which can potentially increase the risk of exposing personal data and breaching confidentiality. AI systems often also need access to personal data which could create a risk if it is not properly secured."

"A number of GCC jurisdictions now have specialist data protection legislation in place. In the Qatar Financial Centre (QFC) data protection is monitored by the Data Protection Office headed by a Commissioner which administers the QFC Data Protections Regulations 2021," Azmeh adds. "A number of these provisions could be particularly relevant when AI is used. Under Article 8 of QFC Data Protections Regulations 2021 data must only be processed for the specific, explicit and legitimate purposes for which it was originally collected and if, say, it was subsequently used to train an AI system without additional consent this would be a breach of the regulations. Those holding personal data must also ensure the information they hold is accurate and not misleading so it will be important to ensure the risk of inaccuracy has not been increased by AI processing. In addition, Article 22 of QFC Data Protections Regulations 2021 includes specific provisions which apply when automated individual decision making (decisions made exclusively without the intervention or involvement of a human) such as a recruitment test which uses pre-programmed algorithms and criteria and profiling which is analyses of aspects of an individual to predict their decisions, preferences and interests occurs."

"The QFC Data Protections Regulations 2021 also require organisations to take an approach called data protection by design which means special

Umar Azmeh,

Registrar, Qatar International Court and Dispute Resolution Centrar

bein
MEDIA GROUP

AN
ORIGINAL
ALWAYS
BEATS A COPY

GIVE OUR GAME THE RESPECT IT DESERVES

#NoToPiracy

🌐 **beinmediagroup.com** 📷 **@beinmediagroup** 𝕏 **@beINMEDIAGROUP** in **bein-media-group**

CLOUD COMPUTING: SUPPORTING DEVELOPMENT

Both the public and private sector in Iraq are showing an increasing interest in using cloud computing. Shahin Yasin of Muayad & Associates explains the legal and regulatory framework which will be required for change to happen there at the same pace as in some other MENA countries.

"Cloud computing is transforming the digital landscape across the world, and Iraq is no different," Shahin Yasin states.

"Under Iraqi law, while there is no explicit definition or comprehensive regulation of cloud computing, it is generally regarded as a service delivery model offering computing resources such as storage, processing power, and applications over the internet."

"This approach eliminates the need for businesses and individuals to maintain physical infrastructure, offering scalability and operational efficiency."

"In the GCC and MENA region, cloud computing adoption is increasing, with governments like those in Qatar, the UAE, and Saudi Arabia leading cloud-first initiatives," Yasin continues.

" In Qatar, for example, the Ministry of Communications has introduced a cloud-first strategy which requires government agencies there involved in new IT or technology refresh projects to assess cloud solutions from government-endorsed providers."

"In Iraq, however, the regulatory framework for cloud computing is still evolving, impacting the pace of development in this field," Yasin explains.

"The Iraqi Ministry of Communications has spearheaded efforts to digitise public services, but without a specialised regulatory framework, these initiatives face limitations."

"Iraqi law lacks specific cloud computing laws, creating challenges for businesses and service providers operating in the country."

DATA PROTECTION LAW

"One of the major challenges faced by potential cloud computing users in Iraq, and also in several MENA countries, involves data residency laws," Yasin explains.

"Under Iraqi regulatory practices, sensitive data, particularly financial information, often falls under strict requirements for local storage to protect national security and citizens' privacy," Yasin explains.

"These data residency requirements are particularly relevant in the financial sector, where entities such as the Central Bank of Iraq mandate that financial data be processed and stored domestically," states Yasin.

"Article 40 of the Iraqi Constitution also guarantees the privacy of communications, including digital information, adding another layer of protection for citizens' data within national borders."

"Consequently, while these laws protect personal data, they may also limit the ability of businesses in the country to fully benefit from international cloud services, given the concentration of major data centres outside the region, including in the USA, Germany, and Japan."

"These limitations could prompt Iraq to consider expanding the numbers of domestic data centres there but may also impact foreign investment, as international providers would face constraints on data transfers."

DATA PROTECTION LAW

"In Iraq, data protection is primarily governed by various general laws, including the Iraqi Constitution, the Iraqi Civil Code (Iraq Law No. 40/1951), and the Penal Code (Iraq Law No. 111/1969), rather than a unified data protection law," Yasin explains.

"Article 40 of the Iraqi Constitution establishes the right to privacy, which indirectly governs data protection for individuals, although it lacks specific guidelines which are tailored for digital data."

"In addition Article 437 and 438 of Iraq Law No. 111/1969 as amended, criminalises the unauthorised disclosure of confidential information, especially by those who are privy to sensitive data as a result of their profession," Yasin adds. "However, the absence of comprehensive data protection legislation in Iraq has led to fragmented interpretations, which often require businesses to develop customised

Shanin Yasin
Senior Associate,
Muayad &
Associates LLC

compliance measures," Yasin adds. "A draft Cyber Crimes Law is currently being considered in Iraq which may introduce some specific digital protections, but at present its exact provisions and the timeline for implementation remain uncertain."

"Having a clear, unified data protection framework in Iraq would enhance cloud adoption, as it would offer clearer guidelines for both public and private entities, and help foster trust in cloud technology."

FINANCIAL DATA

"The financial sector faces additional challenges in utilising cloud services in Iraq," Yasin continues.

"Regulations from the Central Bank of Iraq and other authorities mandate local storage of financial data to ensure data protection and maintain sovereignty over sensitive financial information."

"This requirement aligns with Article 40 of the Iraqi Constitution, which safeguards private communications. These data residency mandates complicate the deployment of global cloud services for financial applications, and require financial institutions in Iraq to carefully balance compliance with operational efficiency."

CYBERSECURITY

"For users of cloud computing, cybersecurity is often a primary concern," Yasin states. "The Iraqi Penal Code and other general protections underscore the importance of safeguarding confidential information, including sensitive data such as medical records or government documents."

"While cybersecurity laws in Iraq are evolving, they currently lack specific provisions addressing cloud computing."

"This gap calls for a regulatory framework that balances data protection with national security considerations."

"Other jurisdictions in the MENA region, such as Qatar, have adopted specific cybersecurity frameworks to enhance cloud computing protection, particularly for major events like the World Cup. Iraq, could also benefit from a similar approach by incorporating cyber standards specific to cloud environments, strengthening security protocols for cloud adoption."

WHAT'S NEXT

"While countries like Qatar, the UAE, and Saudi Arabia are pioneering cloud adoption in the MENA region due to their progressive regulatory frameworks, Iraq is still establishing comprehensive cloud computing regulations," Yasin concludes. "In order to enable Iraq to engage fully in the digital transformation, it will be essential that the next steps are the creation of robust guidelines on cross-border data transfers and a structured data protection law."
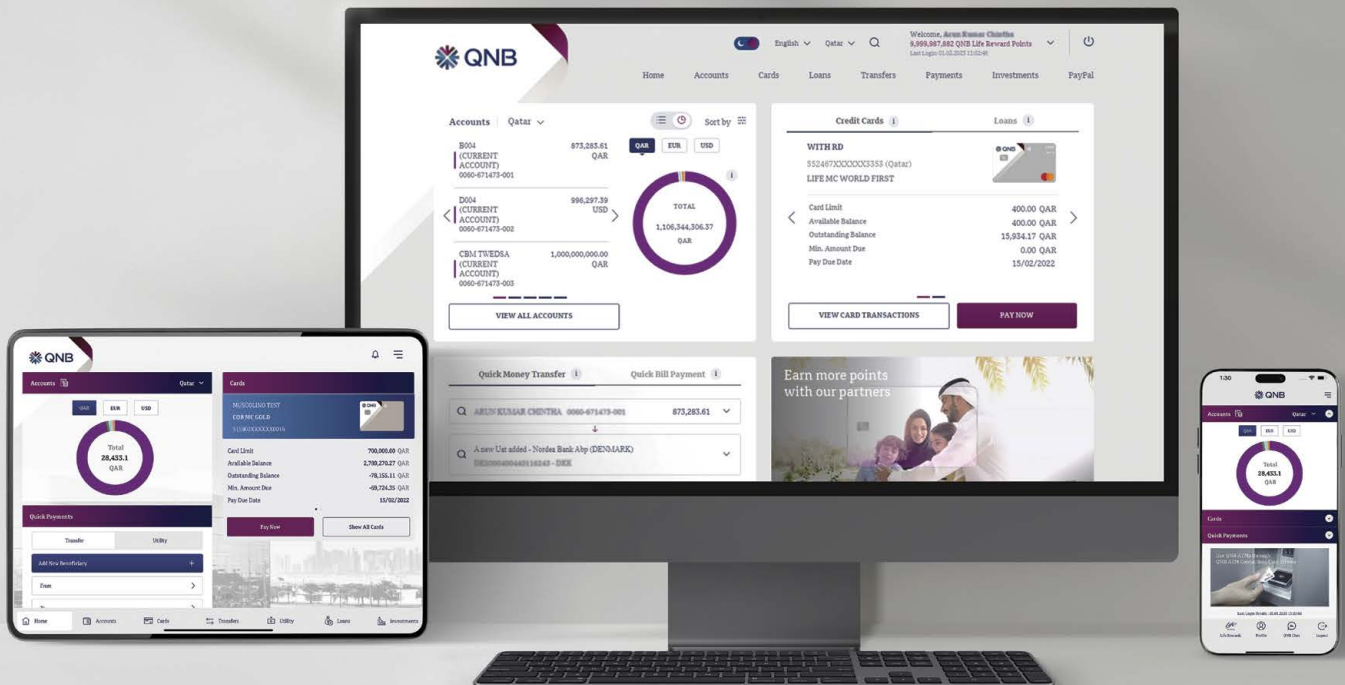
STAR IN YOUR OWN
QATAR AIRWAYS
ADVENTURE

مستقبل الخدمات المصرفية الرقمية يبدأ اليوم
تجربة رقمية سلسة ومبتكرة مع QNB

Tomorrow's digital banking, today
A seamless and innovative banking experience with QNB

qnb.com

ooredoo

Battling to keep communication lines open

Dr Samer Fares, CEO Ooredoo Palestine explains how his team have been working to keep life saving communication lines open in war torn Gaza.

Ooredoo Palestine (OP) has a 20-year 2G and 3G mobile telecommunication licence in the West Bank and Gaza Strip. However, due to Israeli restrictions, OP launched 2G services in the West Bank in 2009 and 3G there in 2018. Since 2017, OP has also operated a 2G network in the Gaza Strip but has not yet received the Israeli approval to operate 3G network. As part of an initiative by the US President to deploy 4G services in Palestine, a memorandum of understanding (MOU) was signed by Israel and the Palestinian Authority in 2022. The execution of the MOU has been very slow, but we hope that the Israel and Palestinian sides will be able to close all the pending points soon to allow OP to launch its 4G services as soon as possible.

CHALLENGES SINCE THE CONFLICT

Since the beginning of the war in Gaza, the Ooredoo team has been working day and night to maintain our 2G network there. During war time telecoms can potentially save lives and, therefore, we treat telecommunications as a humanitarian service. We had to make sure that all our customers in the Gaza Strip have access to telecommunications services so they can reach emergency services, such as medical services and the fire department, as well as family and friends when they need to regardless of their account balance. As a result, from the beginning of the war we put in place a free recurring bundle for all our customers in Gaza. The bundle includes 200 minutes of voice, 300 messages and 50m of data on 2G that allows them to use texting apps such as WhatsApp. OP has also instructed its call centre to provide additional free services to any caller from the Gaza Strip who, for example, is unable to top up their account. Operating a telecom network during a war entails so many risks, most importantly: ensuring the safety and security of our employees, keeping the network operations running and providing continuous support to our customers on the ground. On the employees' side, we are keeping close contact with our employees and we track their movements within Gaza. Furthermore, we provide them with basic support, including financial support, beyond their monthly salaries, and humanitarian support such as, food and tents and other basic needs. Since the beginning of the war, OP has sadly lost four of its employees and OP is providing their families with financial and non-financial support. On the network side, war in Gaza is creating ongoing challenges. As a result of the bombing, the number of active sites in Gaza dropped to around 20% of total network. We have lost 80% of our sites, and our main warehouse. Bombing can occur in any location, at any time, which has kept our technical teams continually having to repair sites and restore services across Gaza. A lack of power has created problems and meant OP has had to secure enough fuel to keep our sites in Gaza operational. OP had to work with the United Nations Relief and Works Agency for Palestine (UNIRWA) to secure the minimum fuel to operate the 20% remaining sites. Moreover, we had to work with the Israeli side to transfer fuel from the South to the North of Gaza as the two areas were separated by an Israeli checkpoint. Due to the war, OP backhaul, which is leased from Paltel, has also faced continuous cuts which have led to blackouts of all our services in the Gaza strip that lasted from a few hours to few days. On customer care, war in Gaza is creating many challenges because we lost most of our show rooms and service centres.

Therefore, we had to think out of the box to make sure that our people in Gaza have ongoing access to our service centres. For this purpose, we had to set up temporary service centres in tents and wooden kiosks and put in place other unconventional customer service tools to reach our displaced customers. With the huge increase in the displaced population, we introduced the Cell-on-Wheels (COWs) concept in Gaza, which has allowed us to move our services with the displaced population and enabled them to access the OP network and services. Last year has been a very tough one for OP in Gaza. However, we have been determined to provide telecom services to Gaza and keep people connected. Telecom services are always important but even more so during wars as they can save lives and contribute to people's welfare. The main lesson I have learnt is that human capital is the most important asset. Our successes would not have been possible without the exceptional work of our team who took personal risks.

BUSINESS NEWS ROUND UP

COVERING NEWS AND DEVELOPMENTS FROM ACROSS OOREDOO GROUP

PARTNERSHIP TO SUPPORT THE MENA AI REVOLUTION

Ooredoo Group has becoming an NVIDIA Cloud Partner (NCP) in order to support its aim to become the leading digital infrastructure provider in the MENA region. Ooredoo is developing an AI-ready platform which is powered by NVIDIA's full-stack innovation across systems, software, and services. In recent years, NVIDIA which is a multinational technology company headquartered in Santa Clara, California has become a dominant supplier of artificial intelligence (AI) hardware and software. The AI platform Ooredoo is building with them will support governments and enable enterprises and start-ups to securely process their private datasets, and also produce valuable insights as tokens that will power innovations for its users.

DATA CENTRES

DIGITAL HUB TO EXPAND

Ooredoo has announced plans to expand its new data centre company, MENA Digital Hub. MENA Digital Hub is a carrier-neutral data centre which is expected to transform the region's digital infrastructure by providing cutting-edge collocation services to hyper-scalers and enterprises. As part of the developments there, Sunita Bottse who was previously the Senior Director of Data Centres Site Acquisition (EMEA) at Microsoft and has also worked in the past for other leading data centre companies, has been appointed CEO of MENA Digital Hub. Ooredoo Group also plans to expand the data centre company's capacity to more than 120 megawatts and has committed to invest over USD 1 billion in the company over the mid to long term. It is expected this expansion will ensure the Group is well positioned to meet the rising regional demand for localised cloud services and IT workloads. Ooredoo Group currently has 26 active data centres across Qatar, Kuwait, Oman, Iraq, and Tunisia, In addition, the Group has

committed to building a new generation of sustainable, energy-efficient, carrier-neutral data centres across its MENA footprint.

FINTECH

WALLETII LAUNCH

Ooredoo Fintech (OFTI) , a wholly owned subsidiary of Ooredoo Group and Ooredoo Oman has launched a new state of the art fintech solution called 'walletii' by Ooredoo - which is Arabic for 'my wallet'. walletii is a user-friendly mobile wallet designed to upgrade and simplify financial transactions for both consumers and merchants. The app's launch is part of Ooredoo's plans to extend the successful Ooredoo Money platform from Qatar to the broader MENA region. walletii is the first mobile money app in Oman to offer a remittance marketplace, and enable users to choose from multiple providers so they can obtain the best rate for their transactions. The walletii app will enable users, whether or not they are Ooredoo customers, to make payments, send and receive money both domestically and internationally, while also earning rewards easily and securely. The app also has chat-like payments which make it more intuitive to use and enable a seamless user experience. walletii users will be rewarded for their everyday transactions through an integrated loyalty programme. The Omani Central Bank has provided Ooredoo with a license to operate the app.

INFRASTRUCTURE

WORLD'S LARGEST SUBSEA CABLE SYSTEM

Ooredoo Oman has signed an agreement to land the 2Africa Cable System in Barka and Salalah in Oman. This will see the most extensive subsea cable landing in Oman to date. The 2Africa Cable System, will span 45,000km, and will be the largest subsea cable system in the world. When it is completed, it will benefit over 3 billion

people in 33 countries on three continents - Africa, Asia, and Europe. The 2Africa consortium is made up of a number of companies including Bayobab, center3, China Mobile International, Meta, Orange, Telecom Egypt, Vodafone Group, and WIOCC. Alcatel Submarine Networks will handle the manufacturing and installation of the cable. The move follows a previously landing of the SMW-5 and TGN Gulf cables in Oman. It is Ooredoo's aim to become the neutral partner of choice for landing submarine cable systems. Salalah was selected as a landing site, as an emerging major new submarine cable landing hub in the south of Oman. The other landing site Barka, is in Muscat. As part of the project Ooredoo Oman will develop a completely new build landing infrastructure at both locations which will be entirely different from any other submarine cable system currently landing in Oman. It is hoped this will help ensure more robust connectivity and access for all operators in Oman.

SUSTAINABILITY

FIRST ESG REPORT SHOWS COMMITMENT TO SUSTAINABILITY

Ooredoo Group has published its first ever standalone Environmental, Social and Governance Report, the GRI-2023 ESG report. The Group has been making ESG disclosures for fou r years but this new standalone report has been developed in line with the latest Global Reporting Initiative (GRI) Universal Standards on reporting as well as the telecoms-specific Sustainability Accounting Standards Board (SASB) standards. The report reveals that as a result of initiatives to optimise network energy usage and transition to energy-efficient technologies in 2023, the total Group direct (Scope 1) and indirect (Scope 2) GHG emissions decreased by 4.5% compared to 2022. In recent years, Ooredoo has launched several renewable energy projects across its operations in order to look at ways of potentially diversifying its energy mix. These have included installing solar panels at key facilities and investing in green energy

solutions which can power its advanced network infrastructure. It was also reported that In 2023, there was a 1.5% increase in female representation across the Ooredoo workforce, bringing the total to 30%. With the support of the Group Human Resources and Sustainability division, Ooredoo is also currently establishing a dedicated ESG committee, which will ensure they take a structured approach to overseeing and guiding sustainability initiatives and performance across the Group..

IN BRIEF

Awards: Deputy Ooredoo Group CEO Sheikh Mohammed Bin Abdulla Al Thani was awarded a Gold Stevie Award in the Most Innovative Leader of the Year category for his achievements during his time as CEO at Ooredoo Qatar at the 2024 Middle East & North Africa Stevie® Awards. These awards recognise innovation in the workplace at all types of organisations in 18 MENA region countries.

Partnerships: Ooredoo Group has agreed a strategic partnership with Dropbox, and has become the first telecommunications company in the EMEA region to offer the company's full suite of business tools to its customers.

PARTNERSHIP
GULF GATEWAY CABLE

Ooredoo Group and e& Carrier & Wholesale, a leading global technology group have partnered to deploy the latest subsea technology which will enable the Gulf Gateway Cable (GGC1) system to be put in place. e& Carrier & Wholesale is the largest internet, mobile and regional hub for international cable systems. The unique solution being worked on by the two companies will provide better latency and enhanced international connectivity and high reliability between their Data Centres in Abu Dhabi and Doha. The deployment of GGC1 will significantly increase existing network capacity, allowing Ooredoo and e& Carrier & Wholesale to offer their customers high-capacity services of up to 28 Tbps with optimal cost and power efficiency per bit. This will enable cost-effective scaling to meet the growing bandwidth demands and enhance network resilience.

TELECOMS
5G DEPLOYMENT

Ooredoo Group has signed a Memorandum of Understanding (MOU) with the global technology company Nokia in order to upgrade business connectivity with cutting-edge 5G solutions. As a result both of these companies will work closely to develop and deploy 5G private networks, delivering innovative market and enterprise-specific solutions which can also be customised in order to meet the diverse needs of businesses in a range of different sectors and industries. In addition, this agreement will allow

Ooredoo business customers to benefit from high-performance, low-latency 5G connectivity.

CHARITABLE WORK
COMMUNITY WORK DURING RAMADAN

This year, staff and business units across the whole Ooredoo Group have been undertaking a number of community initiatives during the holy month of Ramadan designed to help and support the communities the Group is based within. In Qatar, Ooredoo launched 'Endless Giving' which supported a range of community-focused initiatives, including a partnership with the online food delivery company Rafeeq in order to distribute Iftar boxes and sponsor sporting events including the Neshan Ooredoo Ramadan Shooting Championship 2024, the Ekbis Volleyball Championship, and the Al Kass Ooredoo Padel Tournament. The campaign helped customers to contribute to local charities through Nojoom Points donations and provided additional rewards to customers such as double data balances for those travelling to Saudi Arabia for Umrah and access to additional Islamic content channels on Ooredoo tv. Ooredoo Oman launched its 20th Goodwill Journey. The Goodwill Journey has been benefiting the community in Oman for around 20 years. During Ramadan, volunteers travelled across Oman, and worked with local stakeholders to support sustainable change for women, young people, and those with disabilities. The Journey focused on social development, education, digital projects, and empowerment for People and Society, Economy and Development, and Sustainable Environment. The scheme

aimed to upgrade Omani lives and foster sustainable growth through measurable impacts. Ooredoo Kuwait has been working with the Al-Najat Charity in hosting the 'longest Ramadan iftar table' in Kuwait at Souq Al Mubarkiya. Over 1,500 people gathered to break their fast at a table that spread across the entire souq. Food and drinks were offered to seated guests, passers-by and those in need. In Algeria there were also a host of activities taking place during Ramadan including a cultural event, and a renewed commitment to the Algerian Red Crescent (ARC). A food-truck was run with the Ness El Khir foundation, distributing hot meals to those who were fasting and in need. Ooredoo also partnered with the Association Nationale de Volontariat (ANV) on operating a caravan which delivered g essential foodstuffs to underprivileged families in a number of provinces. In addition, over in Tunisia Ooredoo launched the 'Tounes t3ich bellama' which was a scheme which supported Tunisians, especially those who were alone during Ramadan. Initiatives included distributing water and dates to workers observing iftar on the streets, hosting orphans and their supervisors at a memorable iftar, and visiting a retirement home to share iftar and donate health equipment to residents. In addition, support from the digital influencer Mourad Elrouge enabled Ooredoo to distribute iftar boxes to those who were unable to reach their homes in time or lacked means of support. In Palestine Ooredoo worked with organisations such as SOS and Share to help orphans, people in need, and children. Ooredoo Maldives's initiatives focused on the elderly and making intergenerational connections. While in Iraq the company activities included hosting grand Ramadan festivals in Baghdad and Basr and distributing food baskets to 1500 poor families.

Qatar Chamber
Commercial and Industrial Directory
دليل غرفة قطر التجاري والصناعي
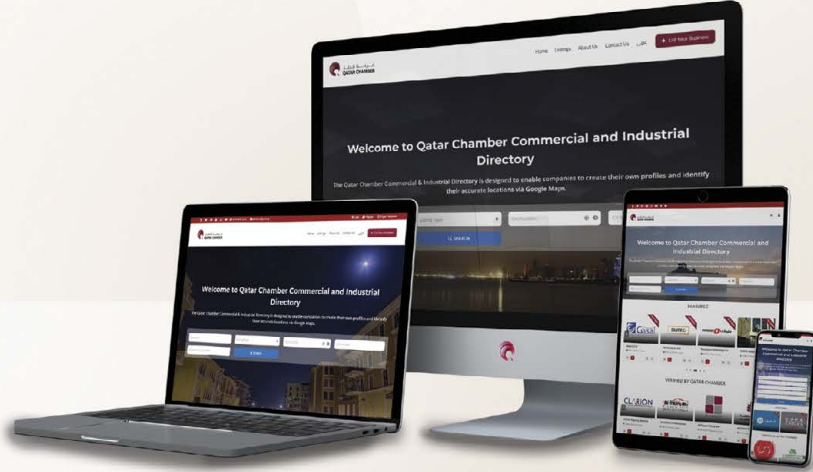
www:// **qatarcid.com**

غــــرفــــة قطـــر
QATAR CHAMBER
www.qatarchamber.com

CYBERSECURITY: THE NEED TO KNOW

Steve Jump of Custodiet explains why understanding what is really important to your own business is key when it comes to cybersecurity.

"In boardrooms across the world cybersecurity is a hot topic as it seems that every aspect of a successful business could potentially be disrupted by a cybersecurity incident," states Steve Jump. "This view is not wrong but it is essential that cybersecurity is no longer assumed by boards as just something for IT to fix. If cybersecurity is to be managed at the level required it can no longer be seen just as a technical problem. Cyber risk must be treated as an existential business risk."

RISKS

"In the digitised world business and systems information infrastructure entirely supports our ability not only to deliver core business functions, but to measure, manage, create, test, protect, and make decisions," Jump adds. "Keeping this infrastructure working and resilient enough to handle business needs is a full-time job that requires diligent, competent, highly technical skills on a 24/7 basis. But as well as having to deal with expected environmental and accidental threats to complex business ecosystems, we also have to contend with adversarial actions of hostile outsiders who want to steal, maliciously destroy or damage our businesses."

"Information Security Management and Cyber Security Management are sometimes seen as equivalent functions," Jump adds.

"They are not. They use similar technology and processes, but the way they support business objectives are different. Information Security Management is about the protection of the value of information as a business asset."

"IT Security is focused on the protection of the information infrastructure itself. Cybersecurity management should be viewed as the implementation of defensive, preventive and corrective processes to prevent hostile attackers from successfully attacking a business. Cybersecurity is an adversarial discipline that requires understanding an enemy."

"Effective, cyber security management cannot just be aligned to achieving business objectives, cyber risk itself must be owned by the business," Jump explains. "To deliver the real business value of correctly and resiliently delivered cybersecurity, cyber risk exposure and impact must be recognised by technical teams implementing it, and management teams funding it. Cybersecurity risk must be discussed and communicated using business value specific terminology so it is truly understood."

"Performance, vulnerabilities and failures not only affect business credibility, but also customers' lives and welfare and the reputation and civil obligations in the countries we and our customers live or operate in. In most jurisdictions any service that collects or uses personal or financial data must protect privacy, which influences required security controls and measures. In many jurisdictions if businesses were aware of a vulnerability that could have led to loss of privacy, financial value or even a life, if ignored, they could become criminally liable or financially liable. However,

KEY POINTS

- Become and remain aware of what really matters to your business.
- Understand threats that could damage what matters to your business.
- Understand what cyber resilience means in terms of risk management and investment.
- Remember you cannot become cyber resilient without being IT resilient.
- Make cybersecurity part of every business case, and change.
- Remember cybersecurity needs to justify its value in terms of risk reduction or avoidance in the same way as any other investment.
- Be able to prove its presence is making a difference.

Steve Jump
Executive Director, Custodiet

being able to prove you have the appropriate technical systems and management controls to ensure privacy is maintained across supply chains and partner networks can be complicated, and even if you have a ISO27000 or equivalent certification, that takes a lot of work, so adding cyber and protective systems into all initial design work is the most economical way of complying."

"Cybersecurity delivery is not cheap, but it can be an extremely expensive item to overlook," Jump states. " It cannot be easily added on when the need is recognised. It must be part of a secure business by design culture. The value of cybersecurity must become integral to every business case, upgrade or design change requirement. Correctly positioned cybersecurity risk impact reduction is a value driven equation, with omission cost exceeding effective implementation costs. To avoid expensive mistakes it must always be considered within a business's own risk context. Simply using the same security systems and technology every other business uses will not guarantee the items that matter most to your business and customers will be protected."

"In today's interconnected world any cyber threat anywhere in the world can be a potential threat in any location," Jump continues. "A new system connected to the internet can expect to be scanned by a bot, active malware, or a hostile actor within seconds of going online. What our cybersecurity practices and business culture present to that scan is the first part of effective cybersecurity management. The successful cyber-attacks which make the headlines are almost always due to basic oversights in configuration or identity management, rather than exotic or complex zero-day exploits so we can to defend against them with minimal additional investment. If we have information or infrastructure of sufficient value, or if an attacker is sufficiently motivated, we can still be directly targeted by a well-resourced attacker. However, we can factor these threats into our risk profile. Not every new threat we read about is a threat we need to technically address. Risk is a combination of a threat AND a vulnerability. Only where both are present do we need to worry. Understanding what matters most in our current business models is where we start. Recognising what an attacker might steal, destroy, or extort is vital. So traditional Political, Economic, Social, Techological, Legal and Environmental (PESTLE) risk modelling is needed. For example, are we most at risk from poor design or poor change management, does our business

deliver products or services criminals might value, and could disruption or destruction of our services politically benefit a hostile adversary. The greatest cyber risk is the assumption we are too small to be of interest to attackers. Most cyber-attacks are not targeted. There is nothing personal about the choice of victim. They result from automated bots scanning. You became a target because an exploitable vulnerability is noted. Every new system and technology deployed has vulnerabilities, we must understand what they may mean in our business context. We need the best cybersecurity protections for these risks and they must be extended or enhanced as necessary. If it becomes too expensive to exploit your company the criminals usually move on to a less expensive victim."

TECHNICAL MEASURES

"There are many technical measures to choose from, and huge sources of information about them but simply having a budget for cybersecurity tools and staff is insufficient. The most powerful technology often requires an understanding of the real business risks to manage, and without this solutions often fail. The key is not just using new technology but effective use of real business risk and measured cybersecurity event data to create better ways of using technology we have, and decide what new technology we need," Jump adds.

"Continuous Threat Exposure Management is a technology that uses your understanding of what really matters to your business and an active, automatically updated Information Asset register where primary value creators in terms of digital, physical and logical value are constantly updated. Then we look at the main threats to this value, vulnerability scans, user activity monitoring, and process and configuration vulnerabilities that may allow those threats to cause harm," Jump continues. "By understanding and mapping every new identified technical vulnerability against only what matters to your business you can greatly improve the accuracy and performance of every part of the cybersecurity systems. Event measurement and monitoring, along with measured and current understanding of threat intelligence in the business specific context, and any actively exploited vulnerabilities in systems, can dramatically reduce the volume of actionable intelligence many tools produce, and allow almost real time views of which risks need urgently addressed now. There is no shortage of new data and event types being detected and stored in Security Information and Event Management (SIEM) databases, but unless the important ones are analysed as soon as they occur, the volume of data may not allow post collection analytics to prevent an attack. Only by making smarter use of live cyber security data and focusing on reducing risks to what matters to our businesses can we reduce the data gap between attackers and defenders. By using our technology to focus on what really matters we can have a managed level of cyber resilience that is within budget and delivers results within our risk appetite."

PROFILE
CHIEF EXECUTIVE OFFICER – QNBN

Qatar's Digital Future

The Qatar National Broadband Network (QNBN) has played an important role in ensuring Qatar has the necessary infrastructure to drive innovation there. Engineer Ahmad Mohamed Al-Kuwari, Chief Executive Officer of QNBN looks at where the Qatari telecommunications sector is headed next.

BACKGROUND

I have a Bachelor of Science in Electrical Engineering from Qatar University and an MBA with Merit from the University of Wales in Cardiff which helped me to learn more about business management. I also completed the Executive Leaders Programme at the Qatar Leadership Centre, which has had a major influence on the way I approach the leadership of dynamic teams which are driving organisational success.

PREVIOUS ROLES AND EXPERIENCE

I have worked for over 22 years in the IT and telecommunications sector. Before joining QNBN where I am now the Chief Executive Officer, I held several leadership roles in different sectors in Qatar.

I was the E-Government Program Manager at the Supreme Council of Communication and Information Technology (ICT-Qatar) which gave me the opportunity to contribute to expanding and improving Qatari online government services. There my focus was enhancing availability, accessibility, and efficiency which led to the streamlining of infrastructure for government-wide processes. This helped me understand how technology can be leveraged to create impactful changes on a national scale.

I was then the CEO of MEEZA, a subsidiary of Qatar Foundation. There I aligned IT services with the Foundation's goals. The focus was on delivering high-quality managed services including data centres, cloud solutions, and looking at cybersecurity.

This helped me better understand how to integrate technology with business strategy to achieve organisational objectives.

My next role was as CEO at Qatar Social Work (QSW), where I led over 1700 employees which gave me more experience of managing larger teams and delivering results which positively impact the community. There the focus was on improving beneficiary satisfaction, employee productivity, and service quality. The scale of this role helped hone these skills.

CURRENT ROLE

As CEO at Qatar National Broadband Network
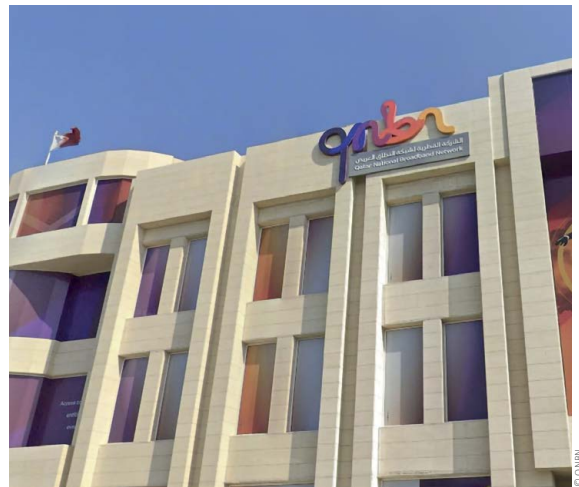
© QNBN

(QNBN), I lead a specialist fibre optics systems team who are developing Qatar's digital infrastructure. My role is to steer the organisation towards continued growth and innovation in the digital connectivity space. I am responsible for overseeing the development and expansion of our passive fibre services, and ensuring we meet the needs of both essential government bodies and private entities in Qatar. From my past roles I have learnt a range of useful lessons including managing large-scale projects and aligning technology with business growth, which have been vital in driving innovation and achieving QNBN's strategic goals. I try to focus on creating customer-centric solutions that not only contribute to Qatar's infrastructure but also enhance user satisfaction.

QNBN OPERATIONS AND ACTIVITIES

QNBN is the leading national passive fibre service provider in Qatar and has put in place high-speed broadband fibre optic infrastructure, which provides fast, reliable, and secure internet and network access to citizens and businesses. Since 2012, QNBN has successfully managed and delivered thousands of connections through the Unified Government Network (UGN), which is the foundation of our business model and its growth.

We have also been expanding our customer base, so it now includes more technically advanced private

sector entities who recognise the benefits of having an unrestricted, unthrottled network, that can provide them with a secure and seamless experience while still reducing costs.

QNBN plays a pivotal role as a critical infrastructure provider in Qatar and facilitates the communications needs of almost all essential government entities. It has become an important asset for the country in the telecom infrastructure sector. Our aim is to leverage this robust foundation so we can further enhance the services we provide and offer an expanded range of options to a more diverse client base. The plan is to strengthen QNBN's position by investing in the expansion of a future-ready, cutting-edge fibre-optic network but we are also continuing to provide our customers with unmatched connectivity, speed, and reliability. Data security and integrity is particularly important to us, and as a result, we are implementing top-tier cybersecurity measures and maintaining the highest industry standards in data protection and integrity.

CRITICAL PROJECTS

At QNBN, I oversee a wide array of critical projects which serve a variety of sectors across Qatar. Currently, we are working on the expansion of fibre connectivity to major entities such as Hamad Medical Corporation (HMC), and are in the middle of Phase III of a project which involves connecting hospitals, key premises and Emergency Medical Services (EMS) centres. We are also currently playing a pivotal role in the development of the Intelligent Transport System (ITS), which is powering key road networks such as Al Majd and Ras Abu Abboud in Qatar.

Our projects cover a whole host of sectors, including government buildings, commercial sites, and public spaces. We are also connecting a growing number of hotels, malls, and other commercial locations. Over 150 connections are planned for completion by the end of 2024 – by mid year we had already completed 60% of these. Our work also includes public infrastructure, and we have ongoing projects which are connecting new parks, beaches, and public plazas.

On the government side, we have been working on connecting new ministry buildings. We also provide connections for a whole range of key clients, including Ooredoo, Alkass, Vodafone, and Qatar Museums, and new clients including banks, and technology and data centre providers are also using our infrastructure. These projects show just how large a volume of work and responsibility QNBN has to manage

SECTORAL CHANGE

Over the next five years, we expect there to be significant changes in Qatar's telecommunications sector, as a result of rapid adoption of cutting-edge technology and an increasing focus on sustainability and cybersecurity. As digital infrastructure continues to expand, concerns about cybersecurity will also increase, and a vigilant approach to protecting data will be needed.

At QNBN, we have been prioritising national security by maintaining a highly secure telecommunications network, and also working closely with the National Cyber Security Agency and other key organisations to implement robust cybersecurity measures. Our use of fibre optic technology plays a critical role in safeguarding data, as it is naturally resistant to electromagnetic interference and can detect any attempts at physical tampering, which makes our network more secure.

In terms of technology, we also expect there will be a shift toward more advanced fibre optics solutions which will offer greater efficiency, speed, and reliability. As these technologies evolve, QNBN is committed to staying at the forefront of innovation, and ensuring investment in our infrastructure can meet the growing demands of the digital landscape. Sustainability will also play a significant role in the sector in the future and as a result QNBN, is focusing on environmental, social, and governance (ESG) principles, in particular on energy efficiency and responsible material sourcing. Our passive optical network design minimises the need for active equipment, which reduces both energy consumption and carbon emissions. Our fibre optic cables are also produced with sustainability in mind, and we continuously implement energy management practices to reduce our environmental footprint. These advances will shape the future of telecommunications in Qatar and help QNBN continue to deliver secure, efficient, and sustainable and cleaner services.

LEGISLATION AND REGULATIONS

The telecommunications sector in Qatar has a strong and collaborative relationship with key governmental bodies, in particularly the Ministry of Communication and Information Technology.

Their guidance has been instrumental in driving forward many initiatives which are shaping digital connectivity in Qatar. The Communication Regulatory Authority (CRA) also plays a vital, supportive role, ensuring our work aligns with national standards and regulatory frameworks.

We are also lucky in that the areas we are working to advance are already being addressed through this collaborative approach.

The close coordination between QNBN, the Ministry of Communications and Information Technology, and the CRA is ensuring that our shared goals—whether these involve cybersecurity, the expansion of fibre-optic networks, or the integration of sustainable practice are also consistently being prioritised and supported by the government and the regulator. It is this strong partnership which enables us to remain agile and forward-thinking, while also continually adapting to the telecommunications sector's and Qatar's evolving needs.

ANY QUESTIONS?

Can personal data leave Saudi Arabia

Ken Wong of CMS looks at the rules governing transfers of personal data outside Saudi Arabia

Saudi Arabia Cabinet Decision No. 98/1443, the Saudi Personal Data Protection Law is now in force along with the Data Transfer Regulations Saudi Arabia Administrative Decision No. 1517/1445 which governs the transfer of Personal Data outside the country's geographical borders. As a result the Saudi Data and AI Authority (SDAIA) has issued a number of new rules and guidelines to help businesses understand the new regime. These include Guidelines for Binding Common Rules (BCRs) For Personal Data Transfer and Standard Contractual Clauses (SCCs) for Personal Data Transfer.

TRANSFERS

The Saudi Personal Data Protection Law allows transfers outside Saudi for a range of purposes including to serve Saudi's national interests and to meet an obligation to which the data subject is a party. In addition, transfers are allowed to achieve what are described as 'other purposes' under the Data Transfer Regulations. These other purposes for transferring or disclosing personal data outside Saudi include: performing necessary operations for central processing to enable the controller to conduct their activities; providing a service or benefit to the personal data subject or conducting scientific research and studies.

SDAIA will publish an official list on its website of countries (and also potentially cities, special economic zones and global trade centres) that provide an appropriate level of protection for data transfers or disclosures outside Saudi. It will be important to check this list regularly as there may be additions and suspensions of the jurisdictions on this list.

OBLIGATIONS

There are conditions that must be met when transferring outside Saudi, which include not causing prejudice to Saudi's national security or vital interests, ensuring the appropriate level of data protection in the destination country, and only transferring the minimum amount of personal data needed. The latter two conditions are exempt (Article 4 Exemption) if any of the following appropriate safeguards are implemented: standard contractual clauses (SCC); binding common rules; or a certificate of accreditation. It should be noted that binding codes of conduct which were previously listed in the superseded data Transfer Regulations as a mitigation are no longer listed.

These appropriate safeguards must include protection of the rights of data subjects, which includes them having the right to file complaints and seek damages for any violations of these rights, even though personal data has been transferred abroad.

Controllers are also required to carry out a risk assessment if the personal data they are transferring outside of Saudi is sensitive data which is going to be transferred on a widespread or continuous basis or it has been transferred or disclosed using an Article 4 exemption.

This differs from the previous provision where a risk assessment had to be conducted where a transfer took place on the basis of an appropriate safeguard or where a controller was unable to rely on an appropriate safeguard and an adequacy decision had not been issued.

BCRS AND SCCS

The Binding Common Rules Guidelines provide instructions on how organisations should prepare these rules. BCRs apply to a 'Group of Entities' (i.e. a set of legal entities engaged in joint economic activity, operating under shared control). In this case all the entities must comply with Saudi Arabia Cabinet Decision No. 98/1443, and its Implementing Regulations. These rules must include the controller's obligations as set out under Saudi Arabia Cabinet Decision No. 98/1443, data subjects' rights and procedures for notifying the competent authority and data subjects if a data breach has occurred. A record of members under the BCRs and of processors and sub-processors must also be maintained. The SCCs which SDAIA have issued are quite similar to those which have been issued by the EU. There are clauses in the case of a controller to processor, controller to controller, processor to controller and processor to processor relationship. It is important to note that any modification of the SCCs will render them invalid, and where the SCCs are incorporated into a contract, the contract's provisions must not conflict with the SCCs. The SCCs also require data importers to submit to Saudi law and comply with and enforce any binding decision under Saudi laws and regulations. Therefore, it will be important personal data importers fully understand the Saudi law and regulations on data protection.

Ben Gibson, and Kate Corcoran also contributed to this article.

Contributor
Ken Wong, Partner
CMS

DIGITAL ECOSYSTEM CONFERENCE

20 November 2024

Legislation and regulation to drive a successful digital economy

ooredoo

ABOUT OOREDOO

Ooredoo Group Vision - Enriching people's digital lives

We are on a mission to empower customers across our global footprint to access and enjoy the best of the Internet in a way that is personal and unique to them.

We continue to invest in our networks to ensure seamless connectivity that caters to our customers' growing digital needs.

We are working as a real digital enabler across our markets and we aspire to help people simplify their lives and enjoy exciting and rewarding digital experiences.

Connecting

We play an active role in our local communities, deploying our reliable, trustworthy networks to deliver relevant services that give you access to the solutions and support you need.

Caring

We make things easy for you. With us, everything is simple and transparent. We respond quickly to your requests, and show concern and respect.

Challenging

We love a challenge because we have an ever youthful spirit, fueling our passion to be the best and enabling us to lead change and innovation to benefit our customers.