Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

TMT
2022

Pakistan: Law & Practice
Yousaf Khosa, Shafaq Rehman,
Rafia Rauf and Saira Khalid Khan
RIAA Barker Gillette

practiceguides.chambers.com

PAKISTAN

Law and Practice

Contributed by:
Yousaf Khosa, Shafaq Rehman, Rafia Rauf and Saira Khalid Khan
RIAA Barker Gillette see p.19

CONTENTS

1. CLOUD COMPUTING

1.1 Laws and Regulations

General Legal Framework

Pakistan currently does not have any general laws imposing limitations on the entrusting of processes or data to the cloud. The Ministry of Information Technology and Telecommunication (MOITT) is in the process of seeking comments from stakeholders on a consultation draft (v.25.08.2021) of a personal data protection bill (PDP Bill) before it is tabled in Parliament. This bill has undergone a few iterations, and the most recent draft appears to incorporate input received from stakeholders on the earlier drafts.

If enacted, the PDP Bill will require that personal data is not transferred to any system located outside Pakistan or not under the direct control of the federal or provincial governments of Pakistan, unless it is ensured that the country where the data is transferred offers personal data protection at least equivalent to that under the PDP Bill. Such data is required to be processed in accordance with the PDP Bill and, where applicable, consent must be given by the data subject.

Other than the Enterprise Technology Governance and Risk Management Framework for Implementation by Financial Institutions (FIs) applicable to the financial sector (discussed below), Pakistan currently does not have codes of conduct imposing limitations on the entrusting of processes or data to the cloud in other industries.

Industries with Greater Regulation

Banking sector

The regulator for the banking sector in Pakistan is the State Bank of Pakistan (SBP). Pursuant to BPRD Circular No 5 of 2017, the SBP has notified a framework titled the Enterprise Technology Governance and Risk Management Framework for Implementation by Financial Institutions (FIs) by 30 June 2018, which was amended by BPRD Circular No 6 of 2019 and BPRD Circular No 4 of 2020.

The framework is required to be integrated with the FI's overall enterprise risk management programme to identify, measure, monitor and control technology risks. However, the framework is not "one-size-fits-all" and its implementation needs to be risk-based and commensurate with the size, nature and types of products/services offered and the complexity of the technology operations of individual FIs. FIs are required to exercise sound judgement in determining the applicable provisions relevant to their technology risk profile while implementing this framework.

The SBP framework set out process and requirements relating to (i) permissible cloud outsourcing arrangements, and (ii) internal controls in cloud outsourcing arrangements.

Permissible cloud outsourcing arrangements

The framework provides that, subject to the policy approved by the board of the FI, FIs can take advantage of all types of cloud service models – including software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) – from domestic and offshore cloud service providers (CSPs), keeping in view that:

- FIs may use cloud services for non-core operations and business support processes such as HR modules, procurement functions, non-production environments, sandboxing, inventory management, supply chain management, office productivity, customer relationship management tools, communication tools, security tools, computation and processing services, data analytics and risk modelling, middleware and payment processing services/platforms; and

- all other banking applications and allied infrastructure – which are used to store and process customers' information relating to deposits, loans and credits, and details of balances and transactions in ledger accounts of customers/borrowers – are not permitted to be placed under cloud-based outsourcing arrangements.

Internal controls in cloud outsourcing arrangements

While entering into outsourcing arrangement with CSPs, an FI is required to ensure that:

- all cloud-based outsourcing arrangements are undertaken through legally binding service level agreements (SLAs);
- their data is encrypted at database level, storage level and during network transmission, and will be logically segregated from other data held by the CSPs;
- the arrangement does not contain a lock-in clause – in the case of an exit from cloud services, an FI will have contractual rights to continue with the arrangement until such time as it is able to switch to a substitute arrangement;
- data transferability and portability from one CSP to another is assured and its purging/deletion in case of exit;
- the CSP complies with the SBP's requirement for provision of data/information relating to the FI's operations; and
- disclosure of its data to any third-party by CSP is prohibited without approval of the FI.

Subcontracting is allowed in outsourcing arrangements with CSPs provided the CSPs comply with all relevant laws and the SBP's regulations.

FIs are also required to ensure that their internal/external auditors and SBP have the right to conduct audit and on-site inspection of the CSP or its subcontractor. Furthermore, there should be no restriction on visits by audit or SBP staff. Where audits cannot be conducted for any valid reason, FIs may rely on internationally recognised third-party certifications and reports made available by CSPs. However, such reliance is required to be supported by an adequate understanding and review of the scope, the methodology applied therein and the ability of third parties and CSPs to clarify matters relating to the audit. These reports must be shared with the SBP as and when required.

The Framework for Risk Management in Outsourcing Arrangements by Financial Institutions, notified by BPRD Circular No 6 of 2019, provides that any outsourcing arrangement outside Pakistan, excluding group outsourcing, will require the SBP's prior approval.

Group outsourcing is defined as an arrangement where financial institutions, including foreign banks' branches, enter outsourcing arrangements including technological support services from their parent institutions/subsidiaries/head offices or other branches of foreign banks/related group entities formulated for providing specialised services to group companies inside or outside Pakistan.

Processing of Personal Data in the Context of the Cloud

While there is currently no general legal framework to address the processing of personal data in the context of the cloud, the PDP Bill does contain provisions which would become relevant, once the same is promulgated.

Since the PDP Bill aims to regulate the processing of personal data, cloud service providers will be required to comply with the provisions thereunder; personal data stored on a cloud may only be processed with the consent of the data subject unless the processing is necessary:

- for the performance of a contract to which the data subject is a party;
- for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by a contract;
- in order to protect the vital interests of the data subject;
- for the administration of justice pursuant to an order of a court of competent jurisdiction;
- for legitimate interests pursued by the data controller; or
- for the exercise of any functions conferred on any person by or under any law.

Furthermore, personal data is not permitted to be processed unless:

- the personal data is processed for a lawful purpose directly related to an activity of the data controller;
- the processing of the personal data is necessary for or directly related to that purpose; and
- the personal data is adequate but not excessive in relation to that purpose.

The PDP Bill also provides that critical personal data will only be processed in a server or data centre located in Pakistan. Personal data, other than that categorised as critical personal data, may be transferred outside the territory of Pakistan under a framework (on conditions) to be devised, and a mechanism for keeping a copy of personal data in Pakistan, which is also to be devised by the National Commission for Personal Data Protection (which is required to be established within six months of the promulgation of the PDP Bill into law).

Additional Compliance Requirements

A person providing cloud computing and/or hosting services may fall within the definition of a "service provider", "social media company" or a "significant social media company" in terms of the Prevention of Electronic Crimes Act 2016 (PECA) and the Removal and Blocking of Unlawful Online (Procedure, Oversight and Safeguards), Rules 2021 (RBUO Rules).

Pertinent definitions appearing in the PECA and RBUO Rules appear below:

- "online information system" means an information system connected with other information systems though internet and any cloud-based content distribution services;
- "service provider" includes a person who:
  - (a) acts as a service provider in relation to sending, receiving, storing, processing or distributing any electronic communication or the provision of other services in relation to electronic communication through an information system;
  - (b) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or
  - (c) processes or stores data on behalf of such electronic communication services or the users of such services;
- "significant social media company" means and includes a social media company with more than half million users in Pakistan or is on the list specially notified by the PTA for this purpose from time to time;
- "social media company" means any person that owns, provides or manages online information system for provision of social media or social network service.

The RBUO Rules have been notified under the PECA and provide that any service provider, social media company, or a significant social media, are required to:

- make available community guidelines for access or usage of any online information system, which community guidelines should easily be accessible and will inform the user

of the online information system not to host, display, upload, modify, publish, transmit, update or share any content in violation of local laws;
- provide to the Federal Investigation Agency (FIA) any information or date or content or sub-content contained in any online information system owned or managed or run by the respective service provider, social media company or social media company, in decrypted, readable and comprehensible format or plain version in accordance with the provisions of PECA; and
- deploy mechanisms to ensure immediate blocking of live streaming through an online information system in Pakistan of any online content particularly related to terrorism, hate speech, pornography, incitement to violence and that is detrimental to national security on receiving intimation from the PTA.

2. BLOCKCHAIN

2.1 Legal Considerations

While blockchain companies have started to emerge in Pakistan, and the government has acknowledged the potential of blockchain technology, currently there is no regulatory framework in place to govern the use of such technology and related services in Pakistan.

In recent news, Pakistan's Customs has partnered with logistics blockchain platform, TradeLens, to digitise supply chains moving in and out of the country and enhance control of trade-based money laundering. Additionally, the Minister of Science and Technology recently addressed a blockchain technology summit, at which he claimed that his ministry had launched blockchain technology pilot projects in three universities, which intend to offer degrees on blockchain technology.

Risks and Liability

The general risks associated with the use of blockchain technology are compromised cybersecurity, breach of privacy (including the breach of personal data) and lack of standardised operating standards. However, given the lack of a legal framework for blockchain technology, the entities involved must carefully assess issues of risk and liability, depending on the specific blockchain solutions or applications in question and the structure of the blockchain, and make provision for the same under contract.

Under BPRD Circular No 3 of 2018 (the "Circular"), the SBP has prohibited the banks and financial institutions it regulates from dealing with cryptocurrencies, which are an application of blockchain technology. However, a constitutional petition has been filed in the High Court of Sindh (the "High Court"), seeking issuance of a direction of appropriate nature so as to nullify the Circular and the implementation of a regulatory framework regarding crypto-assets and crypto-mining in Pakistan. While the final judgment in the foregoing case is yet to be passed, the High Court has passed an interim order recognising the importance of cryptocurrency given that it is swiftly becoming an accepted mode of consideration globally.

Moreover, pursuant to the said interim order, the High Court ordered for a committee to be set up, chaired by the Deputy Governor, SBP, which committee was directed to bring forward recommendations to the Ministry of Finance, as to whether cryptocurrency may be made permissible in Pakistan. The High Court further stated that the foregoing decision is a policy matter and will be decided by the federal government. Hence, the Ministry of Finance and Ministry of Law have been directed to decide whether any recommendations put forward by the aforementioned committee are viable, keeping in view Article 18 of the Constitution of Pakistan (which

relates to the freedom of trade, business or profession). In the meantime, the Director of the Federal Investigation Agency (Cybercrimes), and relevant officers, were also directed to act strictly according to the law in respect of persons who might seek to indulge in cryptocurrency and, if necessary, seek guidance from the SBP.

Pursuant to a further interim order passed in the aforementioned case, the High Court stated that the committee has filed a detailed report pursuant to which the committee has recommended a complete ban on all cryptocurrency and unauthorised operation of crypto exchanges in Pakistan. The High Court has now directed that the said report be shared with the Ministry of Finance and Ministry of Law, which ministries are required to consider the report at joint meetings to reach a final decision on whether or not cryptocurrency is to be allowed in Pakistan in any form and, if so, what the regulatory framework of such business would be.

More recently, the FIA decided to launch a grand crackdown on cryptocurrency dealers and has written a letter to the PTA to shut down 1,600 websites for this purpose, in view of the fact that millions have been purportedly embezzled from Pakistani citizens in digital currency fraud. Apart from shutting down these websites, the FIA has also sought the PTA's assistance in taking action against the people running the websites.

Intellectual Property

While blockchain as a software or database can be registered as an intellectual property under the Copyright Ordinance 1962, intellectual property challenges relating to trade marks, copyrights and patents would be the same as for other electronic and physical business activities, as no specific provisions relating to such technology have been introduced within statute or by way of delegated legislation.

Data Privacy

As stated in **1.1 Laws and Regulations**, there is currently no generally applicable data protection legislation in Pakistan. Given the nature of the technology used for such applications, a blockchain may be distributed over several nodes/servers across various geographic locations. Accordingly, when the PDP Bill is promulgated, the primary issue, with regard to blockchain and distributed ledger technology, will be to determine which persons/entities fall within the ambit of the terms data controller and the data processor.

In view of the fact that data, once entered into a blockchain, cannot be changed, in some cases, it may be difficult to determine the legal basis for the processing of personal data, resulting in the potential use of the data for a different purpose than the purpose originally intended.

Additionally, it may be technically, organisationally and even legally difficult for data subjects to exercise their rights (eg, the right to delete or rectify data), and this may also lead to potential problems in terms of cross-border transfers of personal data.

Service Levels

Pakistan does not have any specific service levels applicable to blockchain technology. These levels will have to be based on how relevant parties negotiate the contractual framework for the implementation and/or utilisation of the blockchain service.

Jurisdictional Issues

Pakistan does not have any laws to regulate blockchain technology. However, since this type of technology is designed to operate over the internet, and because a blockchain is distributed to multiple nodes that may be physically located at various global geographic locations, and potentially spread out across several juris-

dictions, in the event of disputes, it is certain to raise potential choice of law and jurisdictional issues. Contractual frameworks should address choice of law and jurisdiction along with the dispute resolution process.

3. LEGAL CONSIDERATIONS FOR BIG DATA, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

3.1 Challenges and Solutions

Technologies such as artificial intelligence and machine learning, which are at the cutting-edge of computing, have had limited practical application until recently, but have come to pervade daily life in a short span of time, and are galvanising a technological paradigm shift. Business analytics and big data are transforming the way businesses and governments operate. Competing on analytics is the new norm, whereby competitive advantage is defined by turning proprietary and other data sets into insights using advanced algorithms. The advances in big data analytics, machine learning and the use of artificial intelligence in relation thereto, may present a great opportunity for Pakistan.

There is, however, no specific regulatory framework currently applicable in Pakistan that addresses the implementation and/or regulation of big data, machine learning and artificial intelligence, which may be the biggest challenge relating to the implementation of these technologies.

A system or product utilising big data, machine learning and/or artificial intelligence technology is presently treated at par with any other system or product of a similar nature.

4. LEGAL CONSIDERATIONS FOR INTERNET OF THINGS PROJECTS

4.1 Restrictions on a Project's Scope

While internet of things (IOT) projects and services are not subject to specific requirements and do not require a special authorisation, there are certain telecommunications standards which may become relevant depending on the type of device(s) to be used and/or service(s) whose provision is contemplated.

The regulator for the telecommunications sector in Pakistan is the PTA, which was created pursuant to the Pakistan Telecommunication (Reorganisation) Act 1996 (PTA Act). Every licence granted by the PTA to its licensee may contain:

- restrictions as to the types of telecommunication system or telecommunication service to be provided by the licensee, the area and period of operation and the types of telecommunication equipment that may be included in its telecommunication system;
- the obligation to ensure that only terminal equipment which is approved for connection to the telecommunication system in question is so connected; and
- obligations to maintain confidentiality of customer data.

Devices which utilise radioelectric spectrum to transmit and/or receive information require a "type approval" from the PTA, before they can be connected to a public-switched network (further details of this are provided in **8.1 Scope of Telecommunications Rules and Approval Requirements**).

Machine-to-Machine Communications and Data Protection

Pakistan does not have a legal framework that specifically regulates machine-to-machine communications. While sector-specific regulators enforce data protection requirements as part of the law and the terms of the licences granted thereunder, the PECA criminalises the misuse of personal data without consent, and it is therefore important that machine-to-machine communications do not result in the commitment of offences under the PECA. These offences include:

- unauthorised access to information systems or data;
- unauthorised copying or transmission of data;
- interference with information systems or data;
- unauthorised access to critical infrastructure information systems or data;
- unauthorised copying or transmission of critical infrastructure data;
- interference with critical infrastructure information systems or data;
- electronic forgery;
- electronic fraud;
- unauthorised use of identity information;
- unauthorised interception;
- malicious code;
- spamming; and
- spoofing.

Communication Secrecy

The transmission of encrypted data on a public-switched network as traffic is not permitted under the applicable laws. Non-standard protocols of communication, including encryption, cannot be undertaken without prior approval of the PTA. Prior approval of the PTA is required for use of a non-standard mode of communication including virtual private networks (VPN) and non-standard protocols which include encrypted messages. The use of any non-standard of communication, including all mechanisms by means of which communications become hidden or modified to the extent that they cannot be monitored, is a violation of applicable laws.

5. CHALLENGES WITH IT SERVICE AGREEMENTS

5.1 Legal Framework Features

Agreements for provision of IT services are not specifically regulated under Pakistan law, and are therefore subject to be governed according to the volition of the parties in terms of the Contract Act 1872, and are generally reflective of best practices in the sector. This provides parties with the possibility to reflect their interest and will in their legal relationship. A contract, however, may not be contrary to the law in force, and parties may be required to comply with certain obligations, which may result from sector-specific regulations.

Please also refer to the ‘Banking sector’ and the ‘Processing of Personal Data in the Context of the Cloud’ sections in **1.1 Laws and Regulations**.

Foreign Exchange Controls

One of the greatest challenges that local organisations encounter in terms of entering into IT service agreement(s) with non-residents, is in seeking an exemption from the SBP, in connection with the restriction imposed on outward payments to non-residents under the Foreign Exchange Regulation Act 1947 (FERA). Pursuant to the FERA, save as may be provided in and in accordance with any general or special exemption form the provisions of FERA which may be granted conditionally or unconditionally by the SBP, no person in, or resident in, Pakistan is permitted to make any payment to or for the credit of any person resident outside Pakistan.

The SBP has, however, extended a general exemption to the restriction contained in the FERA, whereby scheduled banks have been given a general permission to release foreign exchange up to a maximum of USD100,000 (or its equivalent in other currencies) per invoice for private sector companies incorporated in Pakistan, and those branches of foreign companies which are operating in Pakistan with the permission of the Board of Investment. The foregoing exemption applies when such companies/branches are undertaking permissible business/commercial activities, paying local taxes and periodically repatriating their profits abroad (subject to compliance with relevant provisions of applicable law).

After satisfying themselves of the genuineness of the requests, and after deducting all applicable taxes, the SBP allows the above-mentioned payments for charges on account of utilisation of IT services such as:

- satellite transponder charges;
- international bandwidth charges;
- international internet service charges;
- international private line charges;
- software licence, maintenance or support fees for proprietary/specialised software; and
- subscriptions or payments for access to foreign electronic media and databases.

The SBP has also extended a general permission to scheduled banks to release foreign exchange up to a maximum of USD400,000, or equivalent in other currencies, per year (starting from the date of designation of the relevant scheduled bank), for each company/firm/sole proprietorship incorporated/established in Pakistan on account of commercial payments, pertaining to digital services, in favour of digital service provider companies.

The above permissions are subject to the fulfilment of procedural requirements, set out in the Foreign Exchange Manual (a compendium of permissions granted by the SBP as regard to FERA, from time to time).

6. KEY DATA PROTECTION PRINCIPLES

6.1 Core Rules for Individual/Company Data

Data Protection Legislation

Currently there is no generally applicable data protection legislation in Pakistan. The PDP Bill, if and when enacted, will provide for and regulate the processing of personal data. The PECA criminalises the misuse of personal data (including personal data processed by a third party in its capacity as a service provider) without consent. Industry-specific regulators have data protection requirements, which have been imposed by legislation and in licences granted by them.

Telecom sector

The Pakistan Telecom Rules 2000 (PTA Rules) provide that a licence issued by the PTA will be subject to the PTA Act and the PTA Rules.

Appendix B to the PTA Rules contains general conditions that apply to all licences pursuant to which licensed services are to be provided (the General Conditions). Furthermore, the licence and licensed services will be subject to the conditions as specified in the Schedule 2 annexed to the General Conditions. Pursuant thereto, all licensees of PTA are required to ensure that employees who obtain information about customers of the licensee or other customer's business (customer information) in the course of their employment, observe the code of practice on the confidentiality of customer information. The confidentiality code is required to be prepared by the licensees in consultation with the PTA and

is required to (i) specify the persons to whom customer information may be disclosed without the prior consent of that customer, and (ii) regulate the customer information which may be disclosed without prior consent of that customer.

Banking sector

The SBP requires all banks and FIs to maintain confidentiality of customer information. The Payment Systems and Electronic Fund Transfers Act 2007 (PSEFT) regulates payment systems and electronic fund transfers in Pakistan, and provides standards for protection of consumers and participants. Pursuant thereto, an FI is not permitted to, except as otherwise required by law, divulge any information relating to an electronic fund transfer, affairs or account of its customer, except in circumstances in which, according to the practice and usage customary among bankers, it is necessary or appropriate for an FI to divulge such information, or the consumer has given consent in respect thereof.

Additionally, no person other than an officer or agent appointed by the FI that maintains the account of a consumer may have access through an electronic terminal to information relating to electronic fund transfer, the affairs, or the account of the consumer. The rules governing the operation of individual accounts will be applicable to electronic fund transfers in relation to disclosure of information to third parties.

The Regulations for Payment Card Security, issued under the PSEFT and as notified by the SBP (vide the PSD Circular No 5 of 2016), provide that:

- card service providers are required to ensure the confidentiality of consumers' data in storage, transmission and processing; and
- customer information will not be transferred to an unauthorised storage or access medium.

The PSEFT provides that any FI that wilfully fails to comply with any provision of the PSEFT – or rules, circulars, directions, orders or by-laws issued under the PSEFT – or any provision thereof, will be liable to pay a fine to the SBP which may extend to PKR1 million. In case of a failure to pay the fine, the SBP may suspend or revoke the licence of the service provider or FI concerned. If any amount of fine remains unpaid, it may be recovered as arrears of land revenue.

Distinction between Companies/Individuals

Current legislation does not make a distinction between companies and individuals. The PDP Bill, if and when enacted, will provide protection of personal data only for individuals, whose consent will be required in order for data controllers to process their data.

General Processing of Data

The PDP Bill, if and when enacted, will provide that a data controller is not permitted to process personal data including sensitive personal data of a data subject unless the data subject has given their consent to the processing of that personal data. Notwithstanding the above, a data controller may process personal data relating to a data subject if the processing is necessary:

- for the performance of a contract to which the data subject is a party;
- for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by a contract;
- in order to protect the vital interests of the data subject;
- for the administration of justice pursuant to an order of a court of competent jurisdiction;
- for legitimate interests pursued by the data controller; or
- for the exercise of any functions conferred on any person by or under any law.

However, personal data is not permitted to be processed unless:

- the personal data is processed for a lawful purpose directly related to an activity of the data controller;
- the processing of the personal data is necessary for or directly related to that purpose; and
- the personal data is adequate but not excessive in relation to that purpose.

The key items relating to processing of personal data are:

- notice to data subject;
- non-disclosure of personal data;
- meeting the data security requirements;
- data retention requirements;
- data integrity and access; and
- record keeping.

The PDP Bill, if and when enacted, seeks to establish an authority called the National Commission for Personal Data Protection, which (once established) will have the power to seek information from data controllers in respect of data processing and impose penalties for non-compliance and non-observance of data security practices, and to order a data controller to take such reasonable measures as it may deem necessary to remedy an applicant for any failure to implement the provisions of the PDP Bill once promulgated. Anyone who processes or causes to be processed, disseminates or discloses personal data in violation of any of the provisions of the PDP Bill will be punished with a fine up to PKR15 million; in case of a subsequent unlawful processing of personal data and offence in relation to sensitive date, the fine may be raised up to PKR25 million.

Processing of personal data

The PDP Bill, if and when enacted, will confer on data subjects, among others:

- the right to access personal data;
- the right to correct personal data;
- the right to withdraw consent;
- the right to prevent processing that is likely to cause damage or distress; and
- the right to erasure.

Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes, will be exempt from the provisions of the PDP Bill. Personal data is also exempt from certain provisions of the PDP Bill if it is processed:

- for the prevention or detection of crime or for the purpose of investigations;
- for the apprehension or prosecution of offenders;
- for the assessment or collection of any tax or duty, or any other imposition of a similar nature by the relevant authority;
- in relation to information of the physical or mental health of a data subject or where the application of the provisions of the PDP Bill to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other individual;
- for preparing statistics or carrying out research, such that personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;
- in connection with any order or judgment of a court;
- for the purpose of discharging regulatory functions where the application of the provisions of the PDP Bill to personal data would be likely to prejudice the proper discharge of those functions; or

- for journalistic, literary or artistic purposes, provided that –
  (a) the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material,
  (b) the data controller subject to reasonable grounds, believes that taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest, and
  (c) the processing of personal data in the interests of the security of the state provided that the processing of personal data will not be permitted unless it is authorised pursuant to an express authorisation by the National Commission for Personal Data Protection.

7. MONITORING AND LIMITING OF EMPLOYEE USE OF COMPUTER RESOURCES

7.1 Key Restrictions

There is no specific legislation to address the use by employees of company computer resources. These matters are required to be addressed in the employment agreement between the employer and the employee.

8. SCOPE OF TELECOMMUNICATIONS REGIME

8.1 Scope of Telecommunications Rules and Approval Requirements

The PTA Act and the rules and regulations framed thereunder (the PTA Laws) provide a framework to regulate the operation of telecommunications systems and the provision of telecommunications services. The PTA Act provides that no person is permitted to establish, maintain or operate any telecommunication system or provide any telecommunication service unless they have obtained a licence under the PTA Act.

For purposes of the foregoing:

- "telecommunications system" means any electrical, electromagnetic, electronic, optical or optio-electronic system for the emission, conveyance, switching or reception of any intelligence within, or into, or from, Pakistan, whether or not that intelligence is subjected to rearrangement, computation or any other process in the course of operation of the system, and includes a cable transmission system, a cable television transmission system and terminal equipment; and
- "telecommunications service" means a service consisting in the emission, conveyance, switching or reception of any intelligence within, or into, or from, Pakistan by any electrical, electromagnetic, electronic, optical or optio-electronic system, whether or not the intelligence is subjected to rearrangement, computation or any other process in the course of the service.

Network and Service Provider Obligations

The definitions of the above-mentioned activities are very broad – therefore, the PTA Act could apply to a wide range of entities and services.

Radioelectric spectrum

The PTA is also responsible for dealing with applications relating to the use of radio-spectrum frequency through its Frequency Allocation Board (FAB), which has the exclusive authority to allocate and assign portions of the radio frequency spectrum to the government, providers of telecommunications services and telecommunication systems, radio and television broadcasting operations, public and private wireless operators, and others.

Terminal equipment/type approval

An approval by the PTA will be required before any terminal equipment can directly or indirectly be connected to a public switched network. The PTA may impose certain conditions on the approval, including conditions limiting its connection to specified types of telecommunication systems. The technical standards for terminal equipment and the procedure for approving test equipment, testing any terminal equipment and certifying that it complies with the relevant technical standards has been provided in the Type Approval Technical Standards Regulations 2021.

A type approval granted by the PTA signifies that particular telecommunication equipment is approved for general sale and is suitable to connect with a specific public telecommunication network.

The following categories of equipment require prior type approval from the PTA:

- tracking system devices with SIM/IMEI-based functionality and which transmit location details (eg, vehicle tracking or smart watches with SIM/tracking);
- satellite terminal equipment;
- wireless radio trans/receiver sets with more than 2 MW output power (eg, VHF, HF, UHF and two-way radios);
- terminal devices operating in ISM as defined by PTA ISM band regulations, RFID, SRD, machine-to-machine (M2M), IoT devices within the band and usage conditions prescribed by the Frequency Allocation Board (FAB) of the PTA;
- IP phones, videoconferencing, voice-over internet protocol (VoIP) systems, gateway, etc;
- PABX/IP-PABX;
- SIM/IMEI/Wi-Fi based mobile devices (eg, mobile handsets, Wi-Fi tablets, dongles, wingles).

The following types of equipment are exempted from type approval:

- networking equipment (switches, firewalls, servers, storage devices);
- laptops, desktops and personal computers;
- tablet PCs with Wi-Fi only functionality (non-SIM based devices);
- GPS-only devices.

A non-refundable processing fee of PKR5,000 per application for locally manufactured terminal equipment and USD100 per case for foreign manufactured terminal equipment is charged by the PTA for all new cases, amendment in issued certificate and for issuance of duplicate certificates.

VoIP/instant messaging

Given that transmission of encrypted data on the network as traffic is not permitted under the applicable laws, non-standard protocols of communication, including encryption, cannot be undertaken without prior approval of the PTA. Operators are required to obtain prior approval of the PTA if they use a non-standard mode of communication including VPNs and non-standard protocols which include encrypted messages. Furthermore, the use of any non-standard of communication, including all mechanisms by means of which communications become hidden or modified to the extent that they cannot be monitored, is a violation of applicable laws.

While it is mandatory for service providers to provide local enforcement agencies with decryption and interception abilities for encrypted services, regulation relating to messaging and VoIP is highly topical.

9. AUDIO-VISUAL SERVICES AND VIDEO CHANNELS

9.1 Audio-Visual Service Requirements and Applicability

The Pakistan Electronic Media Regulatory Authority (PEMRA) – established under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (PEMRA Ordinance) – has the mandate to regulate the establishment and operation of all broadcast media and distribution services in Pakistan, established for the purpose of international, national, provincial, district, local or special target audience broadcasting. PEMRA regulates the distribution of foreign and local TV and radio channels in Pakistan.

For the purposes of the foregoing:

- "broadcast media" includes media which originates and propagates broadcast and pre-recorded signals by terrestrial means or through satellite for radio or television, and includes teleporting, provision of access to broadcast signals by channel providers and such other forms of broadcast media as PEMRA may, with the approval of the federal government, specify; and
- "distribution services" includes a service which receives broadcast and pre-recorded signals from different channels and distributes them to subscribers through cable, wireless or satellite options and includes Cable TV, LMDS, MMDS, DTH and such other similar technologies.

Licensing Regime

Operating broadcast media or providing distribution services can only be undertaken once a licence has been obtained from PEMRA. Applications are decided, subject to clearance from the Ministry of Interior and frequency allocation by the Frequency Allocation Board (FAB) in relevant cases. PEMRA issues licences for broadcast media and distribution services for:

- international and national scale stations;
- provincial-scale broadcasts;
- local area or community-based radio and TV broadcasts;
- specific and specialised subjects;
- distribution services; and
- up-linking facilities, including teleporting and DSNG.

PEMRA may also grant permission to a distribution service licensee for the running of an in-house distribution channel subject to such terms and conditions as PEMRA may prescribe, provided that only Pakistani content is permitted to be distributed on such channel.

A licence granted by PEMRA under the PEMRA Ordinance will be valid for a period of five, ten or 15 years subject to payment of the annual fee, as prescribed from time to time. PEMRA may renew a licence on such terms and conditions as may be prescribed and in case of refusal to renew a licence reasons will be recorded in writing. Subject to the terms and conditions of the licence granted by PEMRA, a licensee is not permitted to sell, transfer or assign any of the rights conferred by the licence without prior written permission of PEMRA.

The PEMRA is required to process each application in accordance with prescribed criteria and hold public hearings in the respective provincial capitals of each province or, as the case may be, in Islamabad, before granting or refusing the licence.

Every application form is required to be accompanied by a non-refundable application processing fee as set out in Schedule-B of the Pakistan Electronic Media Regulatory Authority Rules 2009 (PEMRA Rules). Applications for the grant

of a licence will, in the first instance, be short-listed by considering their:

- financial viability;
- technical feasibility;
- financial strength;
- credibility and track record;
- majority shareholding and management control (which should vest in Pakistani nationals);
- prospects of technical progress and introduction of new technology;
- market advancement, such as improved service features or market concepts;
- contribution to universal service objectives; and
- contribution to other social and economic development objectives.

Ownership restrictions

PEMRA will not grant a licence to:

- a person who is not a citizen of Pakistan or resident in Pakistan;
- a foreign company organised under the laws of any foreign government;
- a company the majority of whose shares are owned or controlled by foreign nationals or companies whose management or control is vested in foreign nationals or companies; or
- any person funded or sponsored by a foreign government or organisation.

Foreign Programmes and Local Content Requirement

Licensees of PEMRA, pursuant to the terms of their licence, are required to carry all channels of Pakistan Television Corporation (PTV), the national broadcaster, and all licensed satellite TV and foreign satellite TV channels having landing rights permission from PEMRA. Such licensees, under all circumstances, will provide the "basic service", which includes a range of satellite TV channels as determined by PEMRA, comprising channels with religious, educational, informational, news and entertainment content. A licensee will be restricted to carry or relay only those foreign satellite TV channels that have obtained necessary landing rights permission of PEMRA for "landing" into Pakistani territory. A licensee may not discriminate against any licensed TV channel or landing rights permission holder in offering its broadcast or distribution platform.

Licensees of PEMRA, pursuant to the terms of their licence, are required to offer at least one basic service package (this means the free-to-air television channels of the national broadcasters, non-commercial educational and health-related TV channels licensed by PEMRA, and such other free-to-air television channels as determined by PEMRA to be distributed by a distribution service licensee to its subscribers against a fixed minimum monthly subscription fee) that includes the must-carry channels (ie, the channels of national broadcasters, non-commercial educational channels licensed by PEMRA and such other free-to-air television channels as determined by PEMRA to be distributed by the distribution networks including IPTV networks to its subscribers), for which it does not charge a subscription fee at a rate higher than the maximum fee prescribed by PEMRA.

PEMRA has issued a notification whereby the airing of Indian content has been banned. Further, airing programmes that are a production of international entities requires prior approval from PEMRA. PEMRA has also prohibited the broadcast media or distribution service operator from broadcasting or rebroadcasting or distributing any programme or advertisement if PEMRA is of the opinion that such programme or advertisement is:

- against the ideology of Pakistan;
- likely to create hatred among the people;
- prejudicial to the maintenance of law and order;

- likely to disturb public peace and tranquillity or endangers national security; or
- pornographic, obscene, vulgar or offensive to the commonly accepted standards of decency.

Online Content/Internet-Based Platforms

PEMRA regulates the traditional distribution platforms, whereas the PTA, in addition to PEMRA, jointly regulates internet-based platforms.

PEMRA has provided, on its website, Consultation Paper No Web&OTT/1- 2020 in relation to regulating web TV and over-the-top (OTT) TV; however, there is no specific legal framework to regulate such content, except for the RBUO Rules which allow the PTA to block certain online content and/or the entire online system, if such content is not removed by the service provider or social media company. Please see **1.1 Laws and Regulations** ("Additional Compliance Requirements") for further details.

10. ENCRYPTION REQUIREMENTS

10.1 Legal Requirements and Exemptions

Legal Requirements

While there is no general legal requirement for the mandatory use of encryption techniques on electronic communications and documents, encryption as a cryptographic process of encoding information for confidentiality, integrity and authenticity purposes is subject to the provisions of the Electronic Transactions Ordinance 2002 (ETO). The Certification Council created pursuant to the ETO has the power to grant accreditation to service providers including cryptography services.

The transmission of encrypted data on a public-switched network as traffic is not permitted under the applicable laws. Non-standard protocols of communication, including encryption, cannot be undertaken without prior approval of the PTA. Prior approval of the PTA is required for use of a non-standard mode of communication, including VPNs and non-standard protocols, which include encrypted messages. The use of any non-standard of communication, including all mechanisms by means of which communications become hidden or modified to the extent that they cannot be monitored, is a violation of applicable laws.

Encryption Exemption

The use of encryption does not exempt legal entities from applicable laws. However, it may be noted that, after the promulgation of the PDP Bill, data controllers and/or data processors will be required to implement necessary safeguards so as to ensure protection of personal data of data subjects.

Other Laws

While sector-specific regulators have data protection requirements as part of the law and the terms of the licences granted thereunder – such as the SBP requiring that as part of their cloud outsourcing arrangements, FIs' data is encrypted at database level, storage level and during network transmission and will be logically segregated from other data held by the CSPs – the PECA criminalises the misuse of personal data without consent. Please refer to **4.1 Restrictions on a Project's Scope** for further discussion.

11. COVID-19

11.1 Pandemic Responses Relevant to the TMT Sector

Pursuant to a press release dated 24 March 2021, the PTA stated that it leveraged digital technologies to reach COVID-19 patients, identify COVID-19 clusters and run extensive aware-

ness campaigns to reach users through various telecom networks.

The pandemic also marked a pivotal shift towards the usage of digital platforms for day-to-day activities. Start-ups relating to edtech, healthtech, fintech and e-commerce gained particular significance during lockdowns mandated by the respective provincial governments. Such increased dependence on digital platforms has fostered conversations in regard to promulgation of legislation to facilitate online financial services which would make such services more user-friendly.

RIAA Barker Gillette offers the full range of corporate, commercial and dispute resolution legal services for clients including multinational corporations, financial institutions, non-profit organisations, local companies and government agencies. With ten partners and 54 associates in offices in all the major cities of Pakistan, it is one of the country's largest practices. The firm is well versed in advising domestic and multinational clients, and has extensive experience of complex, cross-border work. With specific reference to TMT matters, it regularly advises both national and international clientele, including Ufone (PTML), Jazz (PMCL), Vimpelcom, China Telecom, Apple, Google, Internet.org, Facebook, WhatsApp, Amazon, Vodafone, Nokia and Oberthur Card Systems. In addition to the support and access to the resources of its offices in London, New York, Dubai, Beijing, and Kabul, RIAA Barker Gillette is the exclusive member firm in Pakistan for Lex Mundi, the world's leading network of independent law firms, with in-depth experience in 100-plus countries worldwide.

AUTHORS

Yousaf Khosa is a partner of RIAA Barker Gillette, based in Islamabad, and is recognised as one of the leading lawyers in Pakistan. He has been involved in the drafting of prominent petroleum laws in the country, and regularly advises clients on their corporate, commercial, labour and taxation matters. He is considered an expert in the telecommunication, oil and gas, and construction sectors in Pakistan.

Shafaq Rehman is a partner at RIAA Barker Gillette, based in Karachi, and advises corporate clients on matters relating to investment, mergers and acquisitions, corporate and regulatory compliance, tax, foreign exchange regulation and labour. She is experienced in drafting, reviewing and negotiating various corporate and commercial contracts, including financing and security documentation. In the wake of Pakistan's recent infrastructure development being undertaken as part of the China Pak Economic Corridor, Shafaq is advising several Chinese stakeholders (in their capacity as lenders or sponsors) in respect of their investments in Pakistan.

Rafia Rauf is a senior associate in the corporate department of RIAA Barker Gillette. She assists the firm's partners in a variety of corporate and commercial matters, including corporate compliance, project finance and tax, telecommunication, and data protection regulations.

Saira Khalid Khan is an associate based in the Islamabad office of RIAA Barker Gillette. She advises local and foreign clients on all aspects of corporate/commercial, regulatory and transactional matters. She has particular expertise in the telecommunications sector, advising national and international telecoms companies operating in Pakistan, and has been involved in a number of major telecoms projects and agreements.

RIAA Barker Gillette

D-67/1
Block 4, Clifton
Karachi
75500
Pakistan

Tel: +92 21 1115 29937
Email: pk@riaabarkergillette.com
Web: www.riaabarkergillette.com/pk/

RIAA Barker Gillette