Pakistan - Cybersecurity

TABLE OF CONTENTS

May 2020

1. GOVERNING TEXTS

1.1. Legislation

Currently, Pakistan has no specific legislation in place addressing cybersecurity, however, the Ministry of Information Technology and Telecommunications has prepared a consultation draft titled, Personal Data Protection Bill 2020 ('the Draft Bill'). The Draft Bill *inter alia* provides for the protection of personal data, the obligations of the data controller and data processor, the rights of data subjects, processing of sensitive personal data, exemptions, the establishment of Personal Data Protection Authority of Pakistan, and complaints and offences.

General legislation:

- Electronic Transactions Ordinance, 2002 ('the Electronic Transactions Ordinance'); and
- Prevention of Electronic Crimes Act, 2016 ('PECA').

Sectoral legislation:

Banking

- Payment Systems & Electronic Funds Transfers Act, 2007 ('the Payment Systems Act');
- State Bank of Pakistan ('SBP') Regulations for Payment Card Security ('Regulations for Payment Card Security');
- SBP Regulations for the Security of Internet Banking ('Regulations for the Security of Internet Banking'); and
- SBP Payment System Department Circular No. 09 of 2018, 28 November 2018 ('Circular No. 09').

Telecommunication

- Telecom Consumers Protection Regulations, 2009 ('the Telecom Consumers Regulations'); and
- Regulations for Technical Implementation of Mobile Banking, 2016 ('the Mobile Banking Regulation').

Health care

- Pakistan Medical and Dental Council ('PMDC') Code of Ethics of Practice for Medical and Dental Practitioners ('Code of Ethics')

The Code of Ethics provides that a physician shall preserve absolute confidentiality on all he/she knows about their patient, even in a circumstance where the patient has died. Similarly, the patient has the right to confidentiality. Violations of the Code of Ethics, by any medical or dental practitioner, constitute professional misconduct liable for disciplinary action.

1.2. Regulatory authority

The Draft Bill provides for the establishment of the Personal Data Protection Authority of Pakistan ('the Authority'). Under the Draft Bill, the Authority shall be responsible for the protection of the interest data subjects and the enforcement of data protection, prevention of any misuse of personal data, promotion of awareness of data protection, and the handling of complaints. The Authority would have executive and judicial powers, including the powers vested upon a Civil Court under the Code of Civil Procedure, 1908 last amended by The Code of Civil Procedure (Amendment) Act, 2020 to decide a complaint or pass any order for that purpose.

1.3. Regulatory authority guidance

As the Draft Bill is at a consultation stage and the Authority is not yet established, there is no guidance on this count. However, the Authority, under Section 48 of the Draft Bill, will be empowered to make the rules with the approval of the Federal Government of Pakistan ('the Government'). The Authority may make rules pertaining to:

- code of conduct and ethics by data processor and data controller;
- compliance of such code;
- consultation with data controller and data processor;
- publicity and enforcement of code;
- interaction and cooperation with international and regional bodies; and
- setting up or to accredit bodies to audit the security measures of the data controller and data processor.

2. SCOPE OF APPLICATION

2.1. Network and Information Systems

The term 'network' is not defined, however 'information system' is defined in Section 2(p) of the Electronic Transactions Ordinance and in Section 2(xx) of PECA, as follows:

'Information system' means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording, or processing information.

Section 13(1)(c) of the Electronic Transactions Ordinance provides that an electronic communication shall be deemed to be that of the originator if it was sent by an information system programmed by, or on behalf of, the originator.

Section 15 of the Electronic Transactions Ordinance provides the source rules for the determination of the time and place of dispatch and receipt of the electronic communication, unless otherwise agreed between the originator and the addressee. The dispatch occurs when the electronic communication enters an information system outside the control of the originator. The receipt of an electronic communication occurs at the time which the electronic communication enters the information system designated by the addressee, or when the addressee retrieves the same from an information system which is not the designated information system. In case the addressee has not designated an information system, the receipt occurs when the electronic communication enters an information system of the addressee.

The place of dispatch or receipt of electronic communication is not dependent upon the place of location of the information system, but, unless otherwise agreed between the originator and the addressee, is the place where originator or addressee ordinarily resides or has his/her place of business.

The provisions of the Electronic Transactions Ordinance are applicable, by virtue of Section 32, notwithstanding the matters being the subject hereof occurring outside Pakistan in so far as they are directly or indirectly connected to information systems within the territorial jurisdiction of Pakistan.

Sections 3 and 5 of PECA provides that unauthorised access and interference with an information system is an offence punishable with imprisonment or a fine, or with both.

Section 27 of PECA provides that any offence, under this law or any other law, shall not be denied legal recognition and enforcement for the sole reason of the offence being committed in relation to or through the use of an information system. Furthermore, reference to 'property' in any law creating an offence in relation to or concerning property shall include information system.

Section 33 of PECA provides the process to be followed by the authorised officer with the seizure of the information system.

2.2. Critical Information Infrastructure Operators

Sections 2(x) and 2(xi) of PECA respectively define 'critical infrastructure' and 'critical infrastructure information system or data' as follows:

'Critical infrastructure' means critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in:

- major detrimental impact on the availability, integrity or delivery of essential services including those services, whose integrity, if compromised, could result in significant loss of life or casualties, taking into account significant economic or social impacts; or
- significant impact on national security, national defense, or the functioning of the state.

Provided that the Government may designate any private or Government infrastructure in accordance with the objectives of subparagraphs (i) and (ii) above, as critical infrastructure as may be prescribed under the Draft Bill.

'Critical infrastructure information system or data' means an information system, program or data that supports or performs a function with respect to critical infrastructure.

Sections 6, 7, and 8 of PECA provide that unauthorised access, copying, or transmission and interference with a critical information system or data is an offence punishable with imprisonment or a fine, or with both.

Section 13(2) of PECA provides that committing electronic forgery in relation to a critical infrastructure information system is on offence punishable with imprisonment or a fine, or with both.

Section 49 of PECA empowers the Government to constitute one or more computer emergency response teams to respond to any threat or attack on any critical infrastructure information system or critical infrastructure data, or any widespread attack on information systems in Pakistan.

2.3. Operator of Essential Services

Not applicable.

2.4. Cloud Computing Services

Not applicable.

2.5. Digital Service Providers

Section 2(zi) of the Payment Systems Act defines the 'service provider' as follows:

A 'service provider' includes an operator or any other Electronic Fund Transfer Service Provider.

Regulation 2(1)(xxviii) of the Mobile Banking Regulation defines 'Third Party Service Provider ('TPSPs') as follows:

'Third Party Service Provider [TPSP(s)]' mean(s) a Class Applications Service Provider for technical support of mobile banking services, licensed by Pakistan Telecommunications Authority and authorized by SBP to provide technical services for channeling, routing, and switching transactions for branchless/mobile banking only. It should be noted that TPSPs shall be for interoperability purpose within branchless banking domain, whereas Payment System Operators (PSOs) and Payment Service Providers (PSPs) shall provide an electronic platform for clearing, processing, routing and switching or electronic transactions under Rules for PSOs and PSPs issued and as amended by State Bank of Pakistan from time to time).

2.6. Other

Not applicable.

3. REQUIREMENTS

3.1. Security measures

Section 2(x) of the Electronic Transactions Ordinance defines the 'security procedure' as follows:

'Security procedure' means a procedure which:

- is agreed between parties;
- is implemented in the normal course by a business and which is reasonably secure and reliable; or
- in relation to a certificate issued by a certification service provider is specified in its certification practice statement for establishing the authenticity or integrity, or both, of any electronic document, which may require the use of algorithms or, codes, identify-

ing words and numbers, encryption, answer back or acknowledgment procedures, software, hardware, or similar security devices.

The Electronic Certification Accreditation Council ('ECAC'), established under Section 18 of the Electronic Transactions Ordinance, is mandated to grant and renew the security procedures of the certification service providers. ECAC grants accreditation to security procedures of those service providers who comply with the criteria for accreditation specified in the relevant regulations.

Section 41(1) of the Electronic Transactions Ordinance provides that no person shall be compelled to disclose any password, key, or other secret information exclusively within his/her private knowledge, which enables his/her use of the security procedure or advanced electronic signature.

Section 8(1) of the Draft Bill provides that the Authority shall prescribe standards to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration, or destruction. Failure to adopt appropriate data security measures attracts the imposition of a fine. All data controllers and data processors are required to adopt necessary security measures within a period of six months from the day the Draft Bill comes into force.

The SBP, through Circular No. 09, instructed all the banks/microfinance banks to carry out an extensive vulnerability assessment and penetration testing to identify potential weaknesses. In addition to internal assessment, the banks/microfinance banks are to arrange an independent third-party review/assessment of their payment systems.

3.2. Notification of cybersecurity incidents

Section 13 of the Draft Bill requires that the data controller report, within 72 hours of a data breach, to the Authority. The exception is where the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subject.

In case the notification is made beyond 72 hours, the notification is to state reasons for the delay.

The notification must contain the following information:

- description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- name and contact details of the data protection officer or another contact point where more information can be obtained;
- likely consequences of the personal data breach; and

- measures adopted or proposed to be adopted by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

For the banking sector, the Regulations for Payment Card Security requires that in case of a security breach, a detailed report is to be submitted within 14 days to the SBP. In addition, the Regulations for the Security of Internet Banking provide that all established security breaches should be reported to the SBP on a quarterly basis. The impact of a security breach on banks' business, systems, applications, and customers is also required to be submitted.

3.3. Registration with a regulatory authority

The Draft Bill empowers the Authority to devise a registration mechanism for data controllers and data processors, and also to formulate a licensing framework for them.

3.4. Appointment of a 'security' officer

The Draft Bill does not have an express requirement to appoint a data protection officer ('DPO') (or a security officer). However, the Draft Bill, while discussing the functions of the Authority, empowers the Authority to formulate compliance framework for monitoring and enforcement with respect to responsibilities of a DPO. It follows that on promulgation of the Draft Law, the Authority shall devise rules for the appointment of a DPO and their responsibilities.

3.5. Other requirements

In Section 45 of the Draft Bill it is provided that any individual or relevant person may file a complaint before the Authority against any violation of personal data protection rights, conduct of any data controller, and data processor of their processes, involving the following:

- a breach of data subject's consent to process their data;
- a breach of the obligations of the data controller or the data processor during the performance of their functions;
- a provision of incomplete, misleading, or false information while taking consent of the data subject; and
- any other matter relating to the protection of personal data.

The Authority is required to provide an answer to the complaint within 30 days of its receipt or within such an extended time, for reasons to be recorded in writing, as reasonably determined by it.

Appeals against the decisions of the Authority are to lie with the High Court or to any other Tribunal established by the Government for the purpose in the manner prescribed by the High Court.

4. SECTOR-SPECIFIC REQUIREMENTS

Cybersecurity in the health sector

Not applicable.

Cybersecurity in the financial sector

Section 70 of the Payment Systems Act provides that a financial institution or any other authorised party shall not divulge any information relating to electronic fund transfer, affairs, or account of its consumer.

Regulation 4.2 (i) of the Regulations for Payment Card Security requires that Card Service Providers shall ensure the confidentiality of consumers' data in storage, transmission, and processing.

Regulation 2.2.3 (c) of the Regulations for the Security of Internet Banking requires that customer information shall not be transferred to unauthorised storage or access medium.

Cybersecurity in the telecom sector

Regulation 16 of the Telecom Consumers Regulations requires that operators (telecom services operators) and their employees shall maintain the confidentiality of information about consumers.

Regulation 5(2)(xxi) of the Mobile Banking Regulations requires that a service-level agreement between third-party service providers, telecom operators, and authorised financial institutions shall be covered in a statement of online privacy that consumer information obtained as a result of mobile banking is collected, used, disclosed, and retained as committed or agreed.

Cybersecurity in the education sector

Not applicable.

5. PENALTIES

Offence	Punishment	Nature
Payment Systems Act		
Any financial institution or service provider who willfully fails to comply with the provisions of the Payment Systems Act or rules, circulars, directions, orders, or by-laws issued under the Payment Systems Act	A fine which may extend to PKR 1 million (approx.€5,708). In case of failure to pay the fine, SBP may suspend or revoke the license of the service provider or the financial institution.	Civil
The Telecom Act		
Contravention of any rules or regulations issued under the Pakistan Telecommunication (Re-organization) Act, 1996 ('the Telecom Act')	Imprisonment for three years or fine of PKR 10 million (approx. €57,080), or both.	Criminal
The Draft Bill		
A data controller not ceasing the processing of personal data after withdrawal of consent by the data subject	Fine up to PKR 5 million (approx. €28,542) or imprisonment for a term not exceeding three years, or both.	Criminal
Anyone who processes or causes to be processed, disseminates, or discloses personal data in violation of the Draft Bill	Fine up to PKR 15 million (approx. €85,627) and in case of a subsequent unlawful processing the fine may be raised up to PKR 25 million (approx.€142,713). In case of sensitive date, the fine may be raised to PKR 25 million.	Civil
Failure to adopt the security measures that are necessary to ensure data security	Fine up to PKR 5 million.	Civil

Failure to comply with the orders of the Authority or the court	Fine up to PKR 2.5 million (approx. €14,270).	Civil
Corporate liability on a legal person	Fine not exceeding 1% of its annual gross revenue in Pakistan or PKR 30 million (approx.€171,255), which-ever is higher.	Civil

PECA

Unauthorised access to information system or data	Imprisonment up to three months or fine up to PKR 50,000 (approx. €285), or with both.	Criminal
Unauthorised copying or transmission of data	Imprisonment up to six months or fine up to PKR 100,000 (approx. €570), or with both.	Criminal
Interference with information system or data	Imprisonment up to two years or fine up to PKR 500,000 (approx. €285), or with both.	Criminal
Unauthorised access to critical infrastructure information system or data	Imprisonment up to three years or fine up to PKR 1 million, or with both.	Criminal
Unauthorised copying or transmission of critical infrastructure data	Imprisonment up to five years or fine up to PKR 5 million, or with both.	Criminal
Interference with critical infrastructure information system or data	Imprisonment up to seven years or fine up to PKR 10 million, or with both.	Criminal
Electronic forgery	Imprisonment up to three years or fine up to PKR 250,000 (approx. €1,427), or with both.	Criminal

Electronic forgery – in relation to critical infrastructure information system or data	Imprisonment up to seven years or fine up to PKR 5 million, or with both.	Criminal
Unauthorised use if identity information	Imprisonment up to three years or fine up to PKR 5 million, or with both.	Criminal
Compensation	The court may, in addition to above punishments, make an order for payment of compensation for any damage or loss caused to the victim.	Criminal

6. OTHER AREAS OF INTEREST

Not applicable.

ABOUT THE AUTHORS

Saifullah Khan

S.U.Khan Associates Corporate & Legal Consultants

Mr. Khan is a Managing Partner at S.U.Khan Associates Corporate & Legal Consultants. He is an international trade lawyer and trade policy expert, has more than twenty years of practical experience in the areas of international trade policy and law advisory, which includes Agreement on Antidumping, Agreement on Subsidies & Countervailing Measures, Agreement on Safeguard Measures, General Agreement on Trade in Services (GATS) and TRIPS. He also practices Anti-trust and Competition Law, E-Commerce, Trade Agreements, issues relating to para-tariff & non-tariff barriers, and Alternate Dispute Resolution mechanisms like Mediation & Arbitration etc. He is a Member of the International Chamber of Commerce (ICC) Pakistan Commission on Alternate Dispute Resolution & Mediation. Mr. Khan has also contributed through his active participation in the Task Force meetings held in connection with the establishment of the Organisation of the Islamic Cooperation (OIC) Arbitration Center in Istanbul, Turkey.

saifullah.khan@sukhan.com.pk

Saeed Hasan Khan

S.U.Khan Associates Corporate & Legal Consultants

Mr. Saeed Hasan Khan is a Partner at S.U.Khan Associates Corporate & Legal Consultants. He commenced his professional career with Deloitte and now has more than twenty years of experience in rendering three-tier taxation services: Advisory-Execution-Litigation. His work experience includes both Value Added Tax (VAT) and Taxes on Income (Corporate Tax/Income Tax). He has been advising clients about the implication of various tax issues on their business, execution & compliance of tax obligations (filings, etc) and representing the clients before various authorities including the appellate authorities. He has assisted the clients during their tax audits conducted by the tax authorities and represented the clients before the authorities conducting the tax audits. He has also carried out system audits of various funded projects and their evaluation as per the grant documents. He has also studied accounting & procurement processes of various entities and has advised modifications therein and has developed finance and procurement manuals.

saeed.hasan@sukhan.com.pk

RELATED CONTENT

GUIDANCE NOTE

Spain - Cybersecurity

LEGAL RESEARCH

Information Sheet on Safe Use of Audio and Video Conferencing Systems

LEGAL RESEARCH

Banking Code of the Republic of Belarus

NEWS POST

Greece: Minister issues opinion on open data use

NEWS POST

Ontario: OSC seeks comments on its key priorities