Jurisdiction	Pakistan
Date	18 July 2022
Law Firm	Kabraji & Talibuddin
Name and Position of the person in charge	Alizeh Bashir, Partner
Contact Information	alizeh.bashir@kandtlaw.com

* We are planning to put the information on our website so that the viewers can reach out to you, directly, and if you don't mind, we will include the above contact information in the report. You may have more than one contact person.

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the **private sector** at the present or in the near future?

In Pakistan, a person's right to privacy is enshrined under Article 14(1) of the Constitution of Pakistan 1973, which states that "the dignity of man and, subject to law, the privacy of home shall be inviolable".

Pakistan does not however, have standalone legislation governing personal data protection, provisions akin to which are contained in the Prevention of Electronic Crimes Act 2016 (the "**PECA**"). We do nonetheless expect that laws will be enacted in the near future, given the introduction of the 'Personal Data Protection Bill 2020' (the "**Bill**"), which has recently been approved by the Federal Cabinet of Pakistan and is expected to be tabled before the Senate and National Assembly of Pakistan in the coming months.

ii. Does your country have a general law concerning protection of personal information in the **public sector** at the present or in the near future?

The Right of Access to Information Act 2017 (the "**RoAI Act**") was promulgated to give effect to the fundamental right of access to information as guaranteed under Article 19A of the Constitution, whereby all citizens shall have access to information held by public bodies. Provincial laws on the subject have also since been enacted, the contents of which are materially the same as the RoAI Act 2017.

The RoAI Act ensures *inter alia* that policies, transactions involving acquisition of property, grants of licenses, privileges made by public bodies, final orders and decisions, and other forms of record are made available to the public. However it also limits the extent to which

the public may be granted such access and particularly provides that any record relating to the personal privacy of any individual, or private documents furnished to a public body, (on the express or implied condition that the information contained in any such documents shall not be disclosed to a third party), shall not be made publicly available.

iii. Does your country have laws concerning protection of personal information **which apply in individual (specific) sectors** at the present or in the near future? (If yes, please describe outline.)

Banking Sector: Payment Systems and Electronic Funds Transfers Act 2007

This law provides for the secrecy of customer information held by financial institutions whereby a financial institution or any other authorized party shall, except as otherwise required by law, not divulge any information relating to an electronic fund transfer, affairs or account of its consumer, except in circumstances where: it is necessary or appropriate for a financial institution to disclose such information according to customary practice and usage in the industry, or if the customer has given their consent. Any violation of or failure to comply with the provisions of this Act is punishable with imprisonment or a financial fine, or both.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I..(please add a reply column as necessary,)

The title of the law： Prevention of Electronic Crimes Act 2016

① The definition of "Personal Information"	There is no specific definition for Personal Information; however, "Identity Information" has been defined as "information which may authenticate or identify an individual or an information system, and enables access to any data or information system."
② The scope in which the law applies	Prevention of unauthorized acts with respect to information systems and related offences, as well as mechanisms for their investigation, prosecution and trial, and international cooperation in this respect.
③ The territorial scope	Pakistan; provided that if personal data is required to be transferred to any system located beyond Pakistan or which is not under

	the direct control of any of the governments in Pakistan, it must be ensured that the country where the data is being transferred, offers personal data protection at least equivalent to the protection provided under the PECA and transferred data must be processed in accordance with the PECA and, where applicable, with consent given by the subject of the data.
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	https://na.gov.pk/uploads/documents/1472635250_246.pdf
⑤ The **effective** date *	19 August 2016

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law： Personal Data Protection Bill 2020

① The definition of "Personal Information"	"Personal data" means "any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller and/or data processor, including any sensitive personal data" "Sensitive personal data" means and "*includes data relating to: access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, and ,passports, biometric data, and physical, psychological and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, or any other information for the purposes of the said law and rules made thereunder*."
② The scope in which the law applies	"*Processing, obtaining, holding, usage and disclosure of data while respecting the rights, freedoms and dignity of natural persons, with special regard to their right to privacy, secrecy and personal identity and for matters connected therewith and ancillary thereto*."
③ The territorial scope	Pakistan

④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	https://moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%202020%20Updated.pdf
⑤ The **effective** date *	The Bill shall come into force after one year from the date of its promulgation or such other date not falling beyond two years from the date of its promulgation, as the Federal Government may determine.

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law： Right of Access to Information Act 2017

① The definition of "Personal Information"	Not defined
② The scope in which the law applies	(i) *"to ensure that the people of the Islamic Republic of Pakistan have improved access to records held by public authorities and promote the purposes of making the Government more accountable to its people, of improving participation by the people in public affairs, of reducing corruption and inefficiency in Government, of promoting sound economic growth, of promoting good governance and respect for human rights"*, and, (ii) *"to provide for a law which gives effect to the fundamental right of access to information, as guaranteed under Article I9A of the Constitution of the Islamic Republic of Pakistan and international law, whereby everyone shall have the right to have access to all information held by public bodies subject only to reasonable restrictions imposed by law for matters connected therewith or incidental thereto"*
③ The territorial scope	The RoAI Act applies to "all public bodies of the Federal Government" of Pakistan.
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	https://na.gov.pk/uploads/documents/1510039254_320.pdf
⑤ The **effective** date *	13 October 2017

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law： Payment Systems and Electronic Funds Transfers Act 2007

① The definition of "Personal Information"	Not defined
② The scope in which the law applies	*"to supervise and regulate Payment Systems and Electronic Fund Transfers in Pakistan and to provide standards for protection of the consumer and to determine the respective rights and liabilities of the financial institutions and other Service Providers, their consumers and participants;"*
③ The territorial scope	Pakistan
④ URL ⑤ (please provide the URL officially posted by the government, English page is preferred, if available)	https://pakistancode.gov.pk/new/UY2FqaJw1-apaUY2Fqa-apaUY2FsaZY%3D-sg-jjjjjjjjjjjj
⑥ The **effective** date *	1 July 2007

* If the law has been amended, please fill in the effective date of the amended law.

ii. If there are any special instructions about the laws, please describe them.

III. OECD Privacy Principles

i. If there are any provisions of law which embody each OECD Privacy Principle in your country, please describe the outlines.

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

This principle means that there should be limits on the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

While this principle is not expressly set out, PECA does provide that any person with dishonest intention, who gains unauthorized access to any information system or data, shall be punished with imprisonment or a fine. This language of the principle is more comprehensively covered under the Bill, which expressly provides that data shall only be collected, processed, and disclosed as necessary and in compliance with the provisions of the Bill. Personal data may be collected for specified, explicit and legitimate purposes and must be adequate, relevant and limited to what is

necessary in relation to the purposes for which the data is processed. The Bill further provides that personal data may only be processed if the data subject has given his/her consent, and further that consent shall be obtained from the data subject for each separate and individual instance where personal data is to be processed.

(b) Data Quality Principle

This principle means that personal data should be relevant to the purposes for which they are to be used, and, to the minimum extent necessary for such purposes, should be accurate, complete and kept up-to-date.

This principle is not included in PECA; however, it is covered under the Bill (which is yet to be enacted) wherein personal data must not be processed unless it is processed for a lawful purpose, is necessary for, or directly related to that purpose, and that the personal data is adequate but not excessive in relation to that purpose. A data controller is required to take adequate steps to ensure that the required personal data is accurate, complete, not misleading, and kept up-to-date, and shall assume liability in the event the foregoing requirements are not followed.

(c) Purpose Specification Principle

This principle means that the purposes for which personal data are collected should be specified not later than at the time of the data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

This principle is not included in PECA; however, the Bill provides that a data controller must provide written notice to the data subject notifying them that his/her personal data (specifying its nature) is being collected, the legal basis concerning such collection, the duration for which the personal data is likely to be processed and retained thereafter, and the purposes for which the personal data is being or is to be collected and further processed. The Bill also specifies that the notice shall be given as soon as reasonably possible i.e., when the data subject is first asked by the data controller to provide his/her personal data, when the data controller first collects the personal data of the data subject, or in any other case, before the data controller i. uses the personal data for a purpose other than the purpose for which the personal data was collected, or ii. discloses the personal data to a third party.

(d) Use Limitation Principle

This principle means that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with (c) Purpose Specification Principle, except:

i) with the consent of the data subject; or

ii) authorized by law.

This principle is not included in PECA; however, it is covered under the Bill (which is yet to be enacted), which states that no personal data be disclosed for any purpose other than (i) the purpose for which the personal data was to be disclosed at the time of collection of the personal data, (ii) a purpose directly related to the purpose referred above, or (iii) to any party other than a third party of a 'class' as specified within the Bill, without the consent of the data subject.

(e) Security Safeguards Principle

This principle means that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

This principle is not included in PECA; however, the Bill expressly requires that personal data remain protected from any loss, misuse, modification, unauthorized or accidental access, or disclosure, alteration, or destruction.

(f) Openness Principle

This principle means that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and address of the data controller.

This principle is not included in PECA; the Bill however provides that a function of the National Commission for Personal Data Protection (the "**NCPDP**") is *inter alia* monitoring technological developments and commercial practices that may affect the protection of personal data, and promoting measures and undertaking research for innovation in the field of protection of personal data. The NCPDP is also

empowered to formulate, approve and implement policies, procedures and regulations for its internal administration, and to formulate a compliance framework for monitoring and enforcement, in order to ensure transparency and accountability, subject to measures which include *inter alia,* privacy, data protection impact assessment, and record maintenance.

(g) Individual Participation Principle

This principle means that an individual should have the right:

i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller holds data relating to him;

ii) to have communicated to him, data relating to him within a reasonable time;
at a charge, if any, that is not excessive;
in a reasonable manner; and
in a form that is readily intelligible to him;

iii) to be given reasons if a request made under subparagraphs (i) and (ii) is denied, and to be able to challenge such denial; and

iv) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

This principle is not included in PECA; however, under the Bill, a data subject is entitled to be informed of whether personal data belonging to him/her is being processed by a data controller and may make a request in writing (upon payment of a prescribed fee), for his personal data which is being processed, a copy of such data in intelligible form. In the event such request cannot be fulfilled, a data controller is required to notify a data subject such reasons, or comply to the extent the data controller is able to. The Bill also provides circumstances under which a data controller may refuse to comply with a data access request, such as *inter alia* if the data controller is not satisfied as to the genuine identity of the data subject requesting the personal data, or if the request lacks important detail in order to assist the data controller in complying with such request, or in the event such request may violate the privacy of another data subject. Furthermore, a data subject is endowed with the right to correct his/her personal data by way of a written data correction request, as well as the right to have his/her data erased, whereby the data controller is obligated to erase such data within 14 days.

(h) Accountability Principle

This principle means that a data controller should be accountable for complying with measures which give effect to the principles stated above.

This principle is not included in PECA; however, it is covered under the Bill (which is yet to be enacted), whereby the NCPDP shall be responsible to protect the interest of the data subject and enforce the protection of personal data, prevent any misuse of personal data, promote awareness of data protection, and shall entertain complaints under the Bill.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

i. Collection Limitation Principle

N/A

ii. Data Quality Principle

N/A

iii. Purpose Specification Principle

N/A

iv. Use Limitation Principle

N/A

v. Security Safeguards Principle

N/A

vi. Openness Principle

N/A

vii. Individual Participation Principle

N/A

viii. Accountability Principle

N/A

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as **comprehensive government access** (e.g. limitation on the authorities' access to personal data for investigation purposes, and the safeguard is the attorney-client privilege) to personal data or **Data Localization (e.g., rules requiring domestic installation and storage of servers and data)**? If yes, please describe them.

Government Access

1. The Qanun-e-Shahadat Order 1984 (the "**Order**")

In Pakistan, certain personal data may be considered public record and therefore may impact the rights of a data subject. Aside from the government having access to such personal data, citizens may also in certain circumstances gain access to personal data of another, for example, in the case of judicial proceedings. The Order is the law of evidence in Pakistan which sets out the rules and practices according to which courts are to record evidence of parties in court proceedings and also sets out which forms of evidence are permissible, including in relation to documentary evidence. The Order allows for what may be considered 'private data' to be made public and has as such divided documents into two categories: public documents and private documents. While the term 'public document' has not been expressly defined, the Order has declared the following types of documents to be 'public documents'. These documents are therefore publicly available and allow for the governments and general public to access or obtain copies of such documents. Public documents include: public records kept in Pakistan of private documents; documents forming part of the records of judicial proceedings; documents required to be maintained by a public servant under any law; and registered documents the execution whereof is not disputed.

Certain other categories of documents deemed 'pubic documents' under the Order, such as those relating to records of government bodies, have not been included above; however, it is pertinent to mention that all other documents which do not fall under the 'public documents' category under the Order are considered 'private documents'.

The Order also provides for safeguards against the dissemination of privileged and/or private data and information of a data subject specifically in respect of professional communications, which may have occurred between such data subject and his/her attorney. The Order provides that communications made to an attorney in the course and for the purpose of his/her employment as an attorney, may not be disclosed. This includes the contents and the condition of any document shared with the attorney during his/her employment and remains a continuing obligation even after the employment has ceased.

2. Personal Data Protection Bill 2020 (the "**Bill**")

The Bill (though it remains to be enacted) provides for wholly safeguarding the personal and sensitive data of a data subject. However it does allow for circumstances in which a data controller may process a data subject's personal data if it is necessary for compliance with any legal obligation to which the data controller is subject, or for the administration of justice pursuant to an order of a court of competent jurisdiction. The foregoing being said, the data controller is also obligated under the Bill to provide notice to the data subject in respect of any data which is to be disseminated for any reason.

3. Income Tax Ordinance 2001 (the "**ITO 2001**")

The ITO 2001 is a federal law relating to all matter pertaining to income tax in Pakistan. A 'public servant', though undefined, has been generally regarded to mean any person employed to act for the service of Pakistan where such person is vested with some portion of the sovereign functions of the Government, to be exercised by him/her for the benefit of the public. A public servant's privacy as regards his/her statements, returns, accounts, and record of any proceedings conducted under the ITO 2001 has been safeguarded pursuant to Section 216 thereof, whereby such information shall be confidential and no public servant may disclose such particulars.

The protection regarding disclosure exists notwithstanding anything contained in the National Accountability Ordinance 1999[1], the Order or Federal Investigation Agency Act

1 The National Accountability Bureau (the "**NAB**") is a federal executive agency of the Government of

19742, both of which provide that in the public interest, personal information shall be disseminated where required, or the RoAI Act (see I, ii, above). However, disclosure of personal data of a public servant, may be required by a body of the Federal Government or of a Provincial Government for the purpose of investigation into the conduct and affairs of any public servant, or to a court in connection with any prosecution of the public servant.

In 2021 a case was filed[3] by Justice Qazi Faez Isa, a Judge of the Supreme Court of Pakistan (the "**Petitioner**") against the President of Pakistan, contesting the allegations that he had omitted to declare in his income tax returns, the properties bought by his spouse and children, in a foreign country. One of the allegations leveled by the Petitioner was the violation of his and his family's right to privacy, as the information about the Petitioner and his family that was available with the Federal Board of Revenue (FBR) (i.e. each of their income tax filings), and each of their personal identification information which was available with the National Database and Registration Authority (NADRA), was freely accessed and such tax and NADRA related personal records were obtained and shared by/with the Asset Recovery Unit (ARU) and the media, in violation of the respective statutory provisions relating to confidentiality and the statutory prohibition on sharing such information.

The Supreme Court considered the matter of surveillance and the illegal collection of evidence in light of *inter alia* Article 14(1) of the Constitution of Pakistan and found that the guarantee under Article 14(1) is for the privacy of the home and does not extend to the tax and property records of either the Petitioner or his family members.

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

---

Pakistan, with the mandate to deal with corruption prevention, raise public awareness and enforce anti-corruption measures. Under the NAB Ordinance, the Chairman NAB, or an officer of NAB duly authorised by him, has been authorized to seize data (including that of a personal nature) during the course of an inquiry or investigation of an offence under the NAB Ordinance.

2 The Federal Investigation Agency (the "**FIA**") is a border control, criminal investigation, counter-intelligence and security agency under the control of the Interior Secretary of Pakistan, tasked with investigative jurisdiction on undertaking operations against terrorism, espionage, federal crimes, smuggling, as well as infringement and other specific crimes. Under the FIA Act 1974, members of the FIA have been empowered to arrest persons and seize property. A member's powers are extended to the duties, privileges, and liabilities as the officers of provincial police have in relation to the investigation of offences under the Code of Criminal Procedure, 1898 or any other law for the time being in force.

[3] Cited as: 2021 PLD Supreme Court 1.

Under PECA, the following authority has been established for carrying out the purposes thereof:

Name: Pakistan Telecommunication Authority

Address: PTA Headquarters, Sector F- 5/1, Islamabad, Pakistan. 44000

Telephone: There are various telephone numbers for division such as Enforcement, Law & Regulation, Commercial Affairs, Cyber Vigilance, Consumer Protection Division etc., all of which are available on the website below.

Website: https://www.pta.gov.pk/en/contact-us

Other information if any:

Under the Bill, the following authority is to be established for carrying out the purposes of the Bill.

Name: Personal Data Protection Authority (PDPA)

Address: Not available.

Telephone: Not available.

Website: Not available.

Other information if any: