

DATA PROTECTION LAWS OF THE WORLD

Pakistan



Downloaded: 20 April 2024

PAKISTAN



Last modified 4 January 2024

LAW

Pakistan currently has not enacted data protection legislation per se similar to data protection legislation enacted in other countries of the world, however the Prevention of Electronic Crimes Act, 2016 (**PECA 2016**) at present serves the same purpose to a certain extent.

Moreover, a draft of the Personal Data Protection Bill 2023 (**PDPB**) has been introduced by the Ministry of Information Technology and Telecommunications with a view to having the same being promulgated into law after public consultation, approval from both Houses of Parliament and receipt of assent from the President of Pakistan.

DEFINITIONS

Definition of personal data

The term *personal data* is defined in PECA 2016 in Section 2(xviii) as *identity information*; means an information which may authenticate or identify an individual or an information system and enable access to any data or information system;

Data; in PECA 2016 is defined in Section 2(xiii) as *data*; includes content data and traffic data;

The use of the word *include*; in the abovementioned definition of *data*; is indicative of the fact that the legislators intended for the definition of *data*; to include content data and traffic data in addition to what the typical dictionary meaning and definition of the word *data*; is.

Hence, identity information means any piece of information that is capable of authenticating or identifying an individual and enable access to any piece of information that may indirectly assist in authenticating or identifying an individual.

On the other hand, the PDPB defines *personal data*; as *any* information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that information or other information in the possession of a data controller and / or data processor, including any sensitive or critical personal data. Provided that anonymized, or pseudonymized data which is incapable of identifying an individual is not personal data;.

For the purpose of clarity, *data subject*; under the PDPB means a natural person who is the subject of the personal data, whereas *data controller*; means a natural or legal person or the government, who either alone or jointly has the authority to decide on the collection, obtaining, usage, or disclosure of personal data.

In addition, the PDPB defines *anonymized data*; as personal data which has undergone the irreversible process of transforming or converting personal data to a form in which a data subject cannot be identified. The PDPB defines *pseudonymisation*; as the processing of personal data in such a manner that the personal data can no longer be attributed to

a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

It must be noted, however, that the PDPB is yet to be promulgated into law and therefore the content of the promulgated legislation may differ from the draft.

Definition of sensitive personal data

PECA 2016 does not differentiate between the terms *personal data*; and *sensitive personal data*; and therefore a piece of information that is considered as *sensitive personal data*; shall be covered under PECA 2016 if the same is capable of being classified as *identity information*; under the aforementioned legislation.

The PDPB however specifically provides a definition of *sensitive personal data*; to mean any personal data relating to: financial information excluding identification number, credit card data, debit card data, account number, or other payment instruments data; health data (physical, behavioural, psychological, and mental health conditions, or medical records); computerized national identity card or passport; biometric data; genetic data; religious beliefs; criminal records; political affiliations; caste or tribe; and an individual's ethnicity.

It must be noted, however, that the PDPB is yet to be promulgated into law and therefore the content of the promulgated legislation may differ from the draft.

NATIONAL DATA PROTECTION AUTHORITY

There is currently no authority specific to data protection in Pakistan. However, section 16(2) of PECA 2016 authorizes the Federal Investigation Agency (*FIA*;) established under the Federal Investigation Agency Act, 1974, along with Pakistan Telecommunication Authority (*PTA*;) established under the Pakistan Telecommunication (Re-organization) Act, 1996, to enforce PECA and to take action against unauthorized access and use of identity information. PECA 2016 also grants other powers to PTA to regulate the access, use, processing and retention of data through promulgating various rules under PECA 2016.

The PDPB provides for the creation of a National Commission for Personal Data Protection (*Commission*;) within six months of the coming into force of the PDPB as law.

REGISTRATION

There is currently no registration requirement.

However, the PDPB, which is yet to be promulgated, confers upon the Commission the power to devise the appropriate registration requirements.

DATA PROTECTION OFFICERS

There is currently no law in force which makes mandatory the appointment of a Data Protection Officer. Alternatively, PECA 2016 provides for the establishment of an investigation agency under section 29, whose *authorized officers*; are granted powers of investigation and cognizance, which may be similar to that of a data protection officer in some capacities. The investigation agency under this provision of PECA 2016 is the Federal Investigation Agency (FIA), authorized through rule 3 of the Prevention of Electronic Crimes Investigation Rules, 2018.

However, the PDPB, which is yet to be promulgated into law, recognizes the existence and role of a Data Protection Officer, which shall be determined by the Commission.

COLLECTION & PROCESSING

Section 16(1) of PECA 2016 (*Section 16(1)*), reproduced below for ease of reference, puts restriction on the collection and procession of personal data without the consent of the person whose personal data is being collected and

processed:

Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both.

The PDPB, in addition, provides for the imposition of an obligation upon the data controller to notify the data subject, in writing, regarding the following: the collection of personal data pertaining to the data subject, along with its description; the legal basis of such data collection and data processing; the retention period; the purpose for such data collection and data processing; information relating to the source of such personal data; information regarding cross border transfer of data; informing the data subject of their rights under the PDPB, including the right to request access to the personal data collected and processed, right to request correction of personal data collected and processed, and provide contact information of the data controller; the choices and means of restricting the processing of personal data; the third parties to whom the personal data may be disclosed; the mandatory or voluntary nature of data collection and data processing; and the consequences of failing to supply mandatory personal data. As per the PDPB, where the processing pertains to critical personal data, the PDPB shall (if implemented in its current form) require the same to be processed in a server or digital infrastructure within Pakistan.

It must be noted, however, that the PDPB is yet to be promulgated into law and therefore the content of the promulgated legislation may differ from the draft.

TRANSFER

Section 16 of PECA 2016 prohibits the transmission of identity information of a person without consent.

Section 4 of PECA 2016 penalizes unauthorized copying and transmission of data with dishonest intentions, with imprisonment up to six months, or a fine up to one hundred thousand rupees, or both.

Section 7 of PECA 2016 penalizes unauthorized copying and transmission of critical infrastructure data with dishonest intentions, with imprisonment up to five years, or a fine up to five million rupees, or both. Under Section 2 of PECA 2016, critical infrastructure data means data that supports or performs a function with respect to a critical infrastructure, namely an asset, facility, system, network or process.

Section 42 of PECA 2016 allows for the Federal Government to transfer data to any foreign government, agency or any international organization for the purposes of investigations or proceedings, and for the collection of evidence concerning offences, upon receipt of a request of the designated investigation agency under PECA 2016.

In addition, Pakistan prohibits data transfers to any country that it does not recognize, including: Israel, Taiwan, Somaliland, Nagorno, Karabakh, Transnistria, Abkhazia, Northern Cyprus, Sahrawi Arab Democratic Republic, South Ossetia and Armenia. This list may change from time to time. Additionally, data transfers to India must be justifiable by the transferor.

Data collated by banks, insurance firms, hospitals, defense establishments and other sensitive institutions may not be transferred to any individual or body without authorization from the relevant regulator on a confidential basis. Such data is further regulated by contractual terms. In certain cases, data may not be transferred without authorization from the data subject.

However, banks and financial institutions must maintain confidentiality in banking transactions.

Similarly, the PDPB, which is yet to be promulgated, proposes prohibiting the transfer of personal data to unauthorized persons or systems. Where the transfer of personal data pertains to a transfer to a territory outside of Pakistan, the PDPB would require the territory where personal data is to be transferred to offer an equivalent degree of personal data protection as that provided for in Pakistan, provided that such data transfer is done in accordance with a framework for the transfer of personal data outside of Pakistan as devised by the Commission.

SECURITY

There are currently no additional data security requirements under the provisions of PECA 2016. However, there are additional requirements under sector specific legislation, such as in the banking and finance sector.

Further, once promulgated, the PDPB would require data collectors and data processors to comply with the standards so prescribed by it for the protection of personal data.

BREACH NOTIFICATION

There is, at present, no requirement to report data breaches to any individual or regulatory body specifically under PECA 2016. However, there are self-reporting requirements under sector specific laws, which may contain the reporting of a breach of personal data.

Additionally, the PDPB would, upon coming into force, require the data controller to notify the Commission regarding any personal data breaches that are likely to result in a risk to the rights and freedoms of the data subject, within 72 hours of knowledge of breach. Moreover, the data processor would similarly be required to intimate any breach of personal data to the Commission, within 72 hours, in the event that the data processor is made aware of such breaches.

ENFORCEMENT

For breaches of provisions of PECA 2016 appropriate relief may be sought through courts of law having jurisdiction in the matter. Specifically, for the breach of personal data and identity information, section 16(2) of PECA 2016 authorizes PTA to secure, destroy, block access to, or prevent transmission of such data if an application is made by the data subject.

Other mechanisms of enforcing data protection also require action by data subjects themselves. An individual may file a complaint with the National Response Centre for Cyber Crime (NR3C) of the Federal Investigation Agency (FIA), which is the law enforcement agency authorized under PECA 2016 and its rules.

Sector specific legislation is enforceable by its respective regulatory or governmental authorities.

Additionally, the PDPB, which is yet to be promulgated, would permit the relevant regulatory authority to exercise all powers required to enable the same to enforce the provisions of the PDPB.

ELECTRONIC MARKETING

The legislation at present does not provide a comprehensive framework to regulate electronic marketing and the processing or transmission of any personal data as a result of electronic marketing. Section 25 of PECA 2016 however prohibits any person from engaging in spamming (including transmission of harmful, fraudulent, misleading, illegal or unsolicited information), though it may be noted that the aforementioned prohibition is only applicable where such spamming is done by a person for a wrongful gain.

Pursuant to the provision of PECA 2016 on spamming, PTA has restricted promotional text messages from telemarketing firms, which now have to provide the recipient with an option to unsubscribe in the promotional message.

ONLINE PRIVACY

PECA 2016 criminalizes unauthorized access to information systems or data, copying or transmission of data and use of identity information. PECA 2016 further criminalizes *offenses against the dignity of a natural person*; including the transmission of information through an information system which *harms the reputation or privacy of a natural person*.

Pursuant to the above, PTA has promulgated the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021. The purpose of these rules is to allow greater regulation of online content which may be argued to hamper an individual's privacy and freedom on online platforms. Under section 3 of PECA 2016, the authority under these rules is PTA, which under these rules has very broad powers to examine, block and remove online content under section 3.

Under section 5, PTA also has the power to issue written directions to a social media service provider, to take any such actions for the removal or blocking of online content as it deems fit, and also prescribe timelines to the service provider for compliance

with such a direction. If the direction is not complied with within the timeline, PTA may take actions against the service provider including degrading or terminating its services and levying penalties as well. Such a direction by PTA will also take precedence over the community guidelines of an individual service provider.

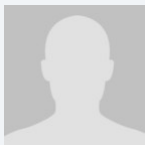
Additionally, an [e-Safety Bill, 2023](#); has been drafted by the Ministry of Information Technology and Telecommunication in Pakistan, for the regulation of online content on social network platforms and service providers.

The bill envisages the establishment of an [e-Safety Authority](#); for enforcing its provisions. This authority shall have various powers to regulate the establishment and registration of and content on social media platforms, to ensure the protection of its users. However, the current discussion draft of the bill contains a broad definition of [data](#); and provides for the access of data to the e-safety authority in a broad and arbitrary provision which allows the authority or any person authorised by it to have access to any communication device for the purpose of searching the device and obtaining any information or data, if it has reasonable cause to suspect contravention of the provisions of this bill. In this manner, the proposed bill may allow another authority access to data on online platforms.

KEY CONTACTS

Liaquat Merchant Associates (LMA)

www.lma.com.pk/



Hira Ahmad

Partner

Liaquat Merchant Associates (LMA)

T +92 21 3583 5101-102-103-104

h.ahmad@lma.com.pk

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.