

CHAPTER 1

PRELIMINARY

1. SHORT TITLE, EXTENT, AND COMMENCEMENT. —

- (1) This Act may be called the Personal Data Protection Act, 2022.
- (2) It shall extend to the whole of Pakistan.
- (3) It shall come into force on such date as the Federal Government may, by notification in the Official Gazette for the commencement of this Act.

2. APPLICATION.—

(1) This Act shall apply —

- a) Where a person collects, processes, discloses, or shares personal data of a data principal whether online or offline within the territory of Pakistan;
- b) Where the State, any Pakistani company, any citizen of Pakistan or any person or body of persons incorporated or created under Pakistani law processes the personal data of a data principal;
- c) Where any data fiduciaries or data processors not having a physical presence within the territory of Pakistan carries out the processing of personal data if such processing is —
 - (i) concerning any commercial or non-commercial activity offering goods or services to data principals; or which involves profiling data principals within the territory of Pakistan.

(2) shall not apply to the processing of anonymised data.

3. DEFINITIONS. — In this Act, unless the context otherwise requires —

- a) “Anonymised data” means personal data which has undergone the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified;
- b) “Biometric data” means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a person, which allow or confirm the unique identification of that person, such as facial images or

dactyloscopy data;

- c) **“Child”** means a person who has not attained the age of eighteen years;
- d) **“Commission”** means the National Commission for Personal Data Protection (NCPDP) established by the Federal government for this Act;
- e) **“Consent”** means any freely given, specific, informed, and unambiguous indication of the data principal wishes by which the data principal, by a statement or by clear affirmative action, signifies agreement to the collecting, obtaining and processing of personal data;
- f) **“Critical personal data”** means data relating to public service providers, unregulated e-commerce transactions and any data related to international obligations;
- g) **“Data”** means any information including but not limited to facts, concepts, and opinions used for communication, interpretation, or processing by humans or by automated means;
- h) **“Data breach”** means the unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data or the loss of any storage medium or device on which personal data is stored in circumstances where unauthorised access, collection, use, disclosure, copying, modification, or disposal of the personal data is likely to occur;
- i) **“Data fiduciary”** means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others has the authority to determine the purpose and means of the processing of personal data;

Explanation: For the purpose of clarity, refer to the “fiduciary” definition in sub-section (l) of section 2.

- j) **“Data processor”** means any person, including the State, a company, any juristic entity, or any individual who alone or in conjunction with others processes personal data on behalf of the data fiduciary;
- k) **“Data principal”** means a person to whom the personal data relates and where such person is a child includes the parents or lawful guardian of such a child;
- l) **“Fiduciary”** means an agent, who has rights and powers normally belonging to another person or to a principal, that must be exercised with a high standard of loyalty and care, for the benefit of the beneficiary or a principal;
- m) **“Financial data”** means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal

or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history;

- n) **"Foreign data principal"** means a data principal who is not a Pakistani national;
- o) **"Genetic data"** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioural characteristics, physiology or health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- p) **"Government"** means the Federal government, the provincial governments and local governments;
- q) **"Harm"** means any harm, whether physical or non-physical, including, without limitation, psychological, financial, or reputational harm, or results in loss of employment or being subjected to blackmailing or sufficiently serious extortion, under the circumstances, or withdrawal of any services, benefit due to an evaluative decision about data principal,
- r) **"Health data"** means any personal data related to the physical or mental health of a data principal including the recordings regarding the past, present or future state or provision of health care services, which may reveal information about his health status;
- s) **"Intersex status"** means the condition of a data principal who is—
 - (i) a combination of female or male;
 - (ii) neither wholly female nor wholly male; or
 - (iii) neither female nor male.
- t) **"Journalistic purpose"** means any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views, or documentaries regarding—
 - (i) news, recent or current events; or
 - (ii) any other information that the data fiduciary believes the public, or any significantly discernible class of the public, to have an interest in;
- u) **"Legitimate interest"** means processing shall be lawful to the extent that at least one of the following applies:
 - (i) Processing is necessary for the legitimate interest pursued by the data fiduciary or by a third party, except where such interests are countermand by the interests or fundamental rights enshrined in the constitution of Pakistan 1973 of an

individual which requires protection of personal data, specifically where a data principal is a child;

- v) **“Loss”** means any loss caused to property of, or otherwise suffered by a person including any loss of profits or loss of use resulting from such damage or destruction and any other loss, direct or indirect, charge, cost, expense, liability, or increased liability howsoever arising suffered or incurred by a person.
- w) **“Person”** includes—
- (i) an individual;
 - (ii) a company;
 - (iii) a firm;
 - (iv) an association of persons or a body of individuals, whether incorporated or not;
- x) **“Personal data breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- y) **“Prescribed”** means prescribed by Rules made under the provisions of this Act;
- z) **“Processing”** means any operation or set of operations carried out about personal data or on sets of personal data, whether by automated means or not, such as recording, collection, organization, adaptation or alteration, retrieval, combination, transmission, erasure or destruction;
- aa) **“Profiling”** means the process of examining, analysing, reviewing, and summarizing data sets to gain insight into aspects concerning the behaviour, attributes or interest of a data principal;
- bb) **“Public interest”** means in the interest of any of the following:
- (i) sovereignty and integrity of Pakistan;
 - (ii) security of the State;
 - (iii) friendly relations with foreign states;
 - (iv) maintenance of public order;
 - (v) preventing incitement to the commission of any cognizable offence relating to the preceding sub-clauses;
 - (vi) preventing the dissemination of false statements of fact.

cc) "Relevant person" means a person concerning data principal:

- (i) who has not attained the age of eighteen years;
- (ii) a natural person authorized by the data principal to access data and/or make data corrections by the parent or a guardian as appointed by a court of competent jurisdiction;
- (iii) if a data principal is incapable of managing his/her affairs, a person shall be appointed by a court to manage the requested affairs request.

dd) "Requestor" means anybody who makes a request under this Act for any matter related or ancillary to this Act;

ee) "Rules" means Rules made under this Act;

ff) "State" shall, unless the context otherwise requires, have the same meaning assigned to it under Article 7 in the Constitution of Pakistan;

gg) "Sensitive personal data" means any personal data revealing, related to, or constituting, as may be applicable—

- (i) Passwords;
- (ii) financial data;
- (iii) health data;
- (iv) official identifier;
- (v) sex life;
- (vi) sexual orientation;
- (vii) biometric data
- (viii) genetic data;
- (ix) transgender status;
- (x) intersex status;
- (xi) caste or tribe;

hh) "Third-party" means a person, public authority, or agency other than the data principal:

- (i) a relevant person about a data principal;
- (ii) a data fiduciary;
- (iii) a data processor;

(iv) a person authorized and under the direct control of a data fiduciary to process personal data.

ii) **“Transgender status”** means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure;

jj) **“Vital interests”** means matters relating to life, fundamental rights, security of a data principal(s), humanitarian emergencies, in particular in situations of natural and man-made disasters, and monitoring and management of epidemics.

4. INTERPRETATION.—

In this Act, unless the context otherwise requires, the following terms shall be read in reference to Rules made under this Act:

- a) the pronouns “he” and “his” has been used throughout this Act for an individual, irrespective of gender.

CHAPTER II

DATA FIDUCIARY OBLIGATIONS

5) GROUNDS FOR PROCESSING PERSONAL DATA. —

- (1) Personal data shall be processed by a data fiduciary in a lawful, and fair manner that respects the privacy of the data principal.
- (2) Personal data shall be processed only for purposes specified, explicit or for any other incidental purposes that are in pursuance of legitimate interest that the data principal would reasonably expect the personal data to be used for and not to be further processed in a manner that is incompatible with those purposes.

6) CONSENT FOR DATA PROCESSING. —

- (1) Data of a data principal shall not be processed unless the data fiduciary seeks his consent, no later than at the commencement of the processing of the data.
- (2) The consent of the data principal under sub-section (1) must be a free, specific,

- informed, and unambiguous indication of the data principal's wishes that signifies agreement to the processing of his data for the specified purpose communicated to him.
- (3) The burden of proof to establish that the data principal has given his consent to the processing of data under this section shall be borne by the data fiduciary.
 - (4) The data principal shall have the right to withdraw his consent to the processing of personal data at any time. The consequences of such withdrawal shall be borne by such data principal. The withdrawal of consent shall not affect the lawfulness of processing the personal data based on consent taken before its withdrawal.
 - (5) Where the data principal withdraws his consent to the processing of personal data under sub-section (4), the data fiduciary shall, within a reasonable time, cease and direct its data processors to cease processing the personal data of such data principal unless such processing can happen without the consent of data principal or authorised under the provisions of this Act or any other law.
 - (6) Notwithstanding sub-section (1), a data fiduciary may process data of a data principal:
 - (a) if the processing is necessary for the performance of a contract to which the data principal is a party;
 - (b) for the taking steps at the request of the data principal to enter into a contract;
 - (c) for compliance with any legal obligations to which the data fiduciary is the subject, other than an obligation imposed by a contract;
 - (d) for protecting the vital interests of the data principal;
 - (e) for treatment, public health, medical or research purposes or to respond to any medical emergency involving a threat to the life or the health of a data principal or any other individual;
 - (f) for compliance with any court order of competent jurisdiction;
 - (g) for the exercise of any functions conferred under any law;
 - (h) for the exercise of any function of the Government authorized by law for the provision of any service or benefit, or the issuance of any certification, license or permit;

(7) A data fiduciary may process the data of a data principal if the processing is necessary for any public interest which may be prescribed by rules.

7) **COLLECTION LIMITATION.**— The sensitive personal data of a person shall only be processed as per the grounds identified in Chapter IV.

8) **NOTICE.** —

- (1) A data fiduciary shall by written notice inform a data principal or where this is not practical, it shall be provided by a data processor of the data fiduciary that exercises control over the same personal data—
- (a) with an itemised notice containing a description and categories of personal data sought to be collected;
 - (b) provide the legal basis for the processing of personal data and the duration for which data is likely to be processed and retained thereafter for further processing;
 - (c) inform the data principal about their rights as mentioned in Chapter V and provide information on contacting the data fiduciary in case of inquiries or complaints concerning personal data;
 - (d) provide the list of third parties to whom the data fiduciary will disclose or may disclose the personal data;
 - (e) the choices and means, the data fiduciary offer the data principal for restricting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;
 - (f) information regarding any cross-border transfer of personal data that the data fiduciary intends to carry out, if applicable;
 - (g) whether it is obligatory or voluntary for the data principal to supply the personal data; and
 - (h) where it is obligatory for the data principal to provide the personal data, but in case of failure to comply with the request, shall face the consequences;
 - (i) any other information as may be specified by the Commission.

2) The notice under sub-section (1) shall be rendered as soon as reasonably possible by the data fiduciary:

- (a) when the data fiduciary requests the data principal to provide data;
- (b) after the data fiduciary collects the personal data of the data principal; or
- (c) in any other case, before —
 - i. using the personal data of the data principal for a purpose other than the one for which the personal data was collected; or
 - ii. discloses personal data to a third party;
 - iii. A notice served under subsection (1) shall be in English or any other language as specified in Article 251 of the constitution of Pakistan, 1973.

9. NON-DISCLOSURE OF PERSONAL DATA. —

(1) Subject to sub-section (6) of section (6), personal data without the consent of the data principal shall not be disclosed

(2) For any purposes other than—

- (a) the purpose for which the personal data was requested; or
- (b) a purpose directly related to the purpose referred to in sub-paragraph (i); or
- (c) the list of third parties as specified by a data fiduciary.

10. SECURITY REQUIREMENTS. —

(1) Given the national interest, the Commission shall prescribe the best international practices for protecting personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction.

(2) A data fiduciary or data processor shall process personal data by employing appropriate technical and organisational security standards to protect the personal data from the incidents mentioned under sub-section (1):

- (a) to the place or location where the personal data is stored;
- (b) to any security measures incorporated into any equipment in which the personal

data is stored;

(c) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and

(d) to the measures taken for ensuring the secure transfer of personal data.

(3) On behalf of a data fiduciary, if a data processor carries out the processing of personal data to protect it from the incidents mentioned in sub-section (1), the data fiduciary must ensure the data processor's compliance with technical and organisational security standards, as prescribed by the Commission.

(4) The data processor is independently liable to ensure compliance with security standards prescribed under sub-section (1).

11. DATA RETENTION REQUIREMENTS.—

(1) The personal data processed for any purpose shall not be kept longer than necessary for the fulfilment of that purpose or as required under the law.

(2) It shall be the duty of a data fiduciary to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed or as required under subsection (1).

12. DATA INTEGRITY AND ACCESS TO DATA.— A data fiduciary shall take adequate steps to ensure that the required personal data is accurate, complete, not misleading and kept up to date concerning the purpose for which the personal data was collected and further processed.

13. RECORD TO BE KEPT BY THE DATA FIDUCIARY.—

(1) A data fiduciary shall keep and maintain a record of each application, notice, request, or any other information concerning the processed personal data. The manner and form in which the record is to be maintained would be determined by the Commission.

(2) The data fiduciary shall apprise the Commission regularly about the type of data they are collecting, and the processing undertaken on the collective data. This shall not apply in situations where data collection is occasional unless the processing results in the infringement of the fundamental rights and freedoms of the data principal, as enshrined in the Constitution of Pakistan.

14. PERSONAL DATA BREACH NOTIFICATION.—

- 1) In the event of a personal data breach, the data fiduciary shall without undue delay and where reasonably possible, not beyond 72 hours of becoming aware of the personal data breach should notify the Commission and the data principal unless the breach is unlikely to result in the infringement of rights and freedoms of the data principal.
- 2) In the event of a delay in notifying personal data breach beyond 72 hours, the notification of a personal data breach shall be furnished to the Commission and the data principal with a valid reason.
- 3) The personal data breach notification shall provide at least the following information: -
 - (a) description of the nature of the personal data breach including where possible the categories and approximate number of data principals and the categories and approximate number of concerned personal data records;
 - (b) name and contact details of the data protection officer or another point of contact from where additional information can be obtained;
 - (c) likely consequences of the personal data breach;
 - (d) measures embraced or proposed to be adopted by the data fiduciary to address the personal data breach, including, where appropriate, measures to mitigate adverse effects.
- 4) The data fiduciary shall maintain a record of all personal data breaches, comprising the facts concerning personal data breaches, their effects, and the remedial action taken.
- 5) After becoming aware of a personal data breach, the data processor shall also follow the requirements of the personal data breach notification provided under this section.

CHAPTER III

PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

15. PROCESSING DATA RELATING TO CHILDREN.—

- 1) Every data fiduciary shall process a child's personal data in such a manner that protects the rights and interests of the child.

- 2) The data fiduciary shall, before processing any personal data relating to a child, verify his age and seek the consent of his parent or relevant person or authorized person having parental responsibility over the child to decide on his behalf.
- 3) The manner for age verification and parental consent under sub-section (2) shall be prescribed by rules to process children's data, taking into consideration:
 - (a) the volume of personal data processed;
 - (b) the proportion of such personal data likely to be that of the child;
 - (c) possibility of harm to the child arising out of the processing of personal data; and
 - (d) such other factors as may be prescribed.
- 4) A data fiduciary shall not process any personal data of a child that is likely to cause him harm, as prescribed under this Act.
- 5) A data fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.
- 6) The provisions of sub-section (1) and (3) shall not apply to the processing of the personal data of a child for such purposes, as may be prescribed in this Act.

16. EXPLANATION.—

- 1) "authorized person" means, a child, a person or a guardian authorized by the court to make a data access or data correction request;
- 2) "parental consent" includes the consent of a lawful guardian, where applicable.

CHAPTER IV

PROCESSING SENSITIVE PERSONAL DATA

17. PROCESSING SENSITIVE PERSONAL DATA BASED ON EXPLICIT CONSENT

- 1) A data fiduciary shall process sensitive personal data if such processing is strictly required for:
 - (a) any official function of the Government, Parliament or any provincial legislature;
 - (b) any legit function of the State that is for the ultimate benefit of the data principal.

18. PROCESSING SENSITIVE PERSONAL DATA IN CONNECTION WITH LAW OR ANY COURT ORDER. —

- 1) A data fiduciary shall process sensitive personal data if such processing is:
 - (a) for, or in connection with any legal proceedings, or any law enacted by the parliament or any provincial legislature; or
 - (b) to establish, exercise or defend legal rights; or
 - (c) to comply with the orders of any court or Tribunal in Pakistan.

19. PROCESSING SPECIFIC CATEGORIES OF SENSITIVE PERSONAL DATA. —

- 1) A data fiduciary shall process sensitive personal data such as passwords, financial data, health data, official identifiers, genetic data, and biometric data if such processing is strictly for the following purposes —
 - (a) for medical reasons and is undertaken by a healthcare professional to respond to any medical emergency involving a threat to the life or the health of a data principal;
 - (b) to provide urgent medical care or health services to any individual during a pandemic, epidemic, or any other threat to public health; or
 - (c) to ensure the safety of, or aid or services to, any individual during any disaster or any breakdown of public order.

20. FURTHER CATEGORIES OF SENSITIVE PERSONAL DATA.—

- 1) The Commission may notify further categories of personal data as sensitive personal data as deemed fit.
- 2) The Commission may also notify further categories of personal data as sensitive personal data requiring additional protections or restrictions where repeated, continuous, or systematic collection for profiling takes place.

CHAPTER V

DATA PRINCIPAL RIGHTS

21. RIGHT OF ACCESS.—

- 1) A data principal shall have the right to obtain from a data fiduciary confirmation whether the personal data of a data principal is under processing or has been processed by or on behalf of the data fiduciary.
- 2) The data fiduciary shall provide the requested information under sub-section (1) clearly and concisely that is easily comprehensible to a person:
 - (a) A requestor may, upon payment of a prescribed fee, make a data access request in writing to the data fiduciary for the information requested under sub-section (1).

22. RIGHT TO CORRECTION.—

- 1) A data principal shall have the right to correct his personal data obtained by the data fiduciary concerning the purposes for which it is being processed if the requestor considers that the personal data is:
 - (a) inaccurate or misleading;
 - (b) incomplete; and
 - (c) to be updated that is out of date.
- 2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with the need for such correction, completion or updating concerning the purposes of the processing, therefore, the data fiduciary shall furnish the data principal with adequate justification in writing for rejecting the application.
- 3) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (2), the data principal may require that the data fiduciary shall take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal.
- 4) Where the data fiduciary corrects, completes, or updates data under sub-section (1), the data fiduciary shall also take reasonable steps within time as may be prescribed to notify all relevant

entities or individuals to whom such data may have been shared regarding the relevant correction, completion or updating.

23. RIGHT TO DATA PORTABILITY.—

(1) The data principal shall have the right to receive the personal data from the data fiduciary in a structured, commonly used, and machine-readable format and the data principal shall have a right to transmit that data to another data fiduciary without hindrance where technically feasible.

(2) Sub-section (1) shall only apply where the processing is carried out by automated means, and shall not apply:

- (a) where processing is necessary for the performance of a task carried out in the interest of the public;
- (b) where compliance with the law or any court order is mandatory; and
- (c) where it is not technically feasible or by complying with the request under subsection (1) may result in the revealing of a trade secret of any data fiduciary.

24. RIGHTS OF FOREIGN DATA PRINCIPAL.— The foreign data principal residing in Pakistan shall have all his rights under this act where his data has been collected.

25. RIGHT TO ERASURE.—

(1) The data principal shall have the right to request the data fiduciary the erasure of personal data concerning him without undue delay, therefore, the data principal shall have the obligation to erase personal data within a period of 14 days where one or more of the following condition applies:

- a) the personal data are no longer necessary concerning the purposes for which they were collected or otherwise processed;
- b) the data principal withdraws consent on which the processing is based under sub-section (1) of section 26 and where there is no other legal ground for the processing; or
- c) the data principal objects to the processing under sub-section (2) of section 26;
- d) the data have been unlawfully processed; or
- e) the data must be erased in compliance with a legal obligation.

(2) Where the data fiduciary has made the data public and is obliged under subsection (1) to erase the personal data, the data fiduciary shall take adequate steps to erase such data.

(3) Without prejudicing the rights of the person protected under the Act, subsections (1) and (2) shall not apply to the extent that processing is necessary:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation or the performance of a task carried out in the public interest;
- c) for reasons of public interest in the area of public health;
- d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as the right referred to in subsection (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- e) for the establishment, exercise, or defence of legal claims.

26. WITHDRAWAL OF CONSENT.—

- (1) A data principal may, by notice in writing withdraw his consent to the processing of his personal data.
- (2) The data fiduciary shall, upon receiving the notice under subsection (1), shall cease the processing of personal data.
- (3) The withdrawal of the consent shall not affect the lawfulness of the processing based on consent before its withdrawal.
- (4) The failure of the data fiduciary to comply with sub-section (2) shall be construed as an offence and convicted, therefore, liable to a fine that shall be determined as per the discretion of the Commission.

27. RIGHT TO NOMINATE.— In the event of the death or disability of the data principal, he shall have the right to nominate, any other individual as may be prescribed, to exercise the rights of the data principal under the provisions of this Act.

Explanation: For this section, “disability” means the inability to engage in any substantial gainful activity because of any medically determinable physical or mental impairment which can

be expected to result in death, or which has lasted or can be expected to last for a continuous period of not less than 12 months.

28. RIGHT TO REDRESSAL OF GRIEVANCE.—

(1) In case of any complaint/grievance of the data principal, he shall be provided with means to register his complaint in writing with a data fiduciary. The data fiduciary officials shall immediately take up the matter for redressal.

(2) In the case where a data fiduciary fails to satisfy a data principal with a satisfactory response concerning a grievance or receives no response within the prescribed period, he may register a complaint with the Commission in such manner as may be prescribed.

29. RIGHT TO AVOID REPEATED COLLECTION.—

Where a data fiduciary—

(1) has complied with the requirements of this Act concerning the collection of personal data from the data principal, referred to as the “first collection”, and on any subsequent occasion again requests to collect personal data from the same data principal, referred to as the “subsequent collection”, the data fiduciary shall not be required to comply with the requirements of section (9) concerning the subsequent collection if—

- a) to comply with those provisions concerning the subsequent collection means to repeat, in the same circumstances, which was done to comply with that principle in respect of the first collection; and
- b) not more than twelve months have elapsed between the first collection and the subsequent collection.

(2) To avoid ambiguity for this Act, it is asserted that subsection (1) shall not be exercised to prevent a subsequent collection from becoming the first collection if the concerned data fiduciary has complied with the provisions of the notice and consent concerning the subsequent collection.

CHAPTER VI

TRANSFER OF PERSONAL DATA OUTSIDE PAKISTAN

30. RESTRICTIONS ON TRANSFERRING PERSONAL DATA.—

- (1) Every data fiduciary shall ensure personal data is stored on a server or data centre based in Pakistan.
- (2) The Commission shall notify such categories of personal data as critical personal data, from time to time, which shall not be transferred to any other territory outside Pakistan if not authorized by the Government.
- (3) Notwithstanding, anything contained in subsection (1), the Commission may notify certain categories of personal data as exempt from the requirement under subsection (1) on the grounds of public interest, necessity, or strategic interests of Pakistan.

31. CONDITION FOR CROSS-BORDER TRANSFER OF PERSONAL DATA.—

- (1) Where personal data is required to be transferred beyond the borders of Pakistan to an entity/entities or system that is not under the direct control of the Government of Pakistan, the data fiduciary or a processor shall ensure that the country where the data is being transferred offers at least equivalent level of protection of personal data provided under this Act.
- (2) Any Personal data other than those categorised as sensitive personal data may be transferred outside the territory of Pakistan under the conditions to be devised by the Commission.
- (3) The Commission shall also devise a mechanism for keeping some components of the sensitive personal data in Pakistan to which this Act applies, on the grounds of public interest or national security.

32. EXEMPTION.—

- 1) Subject to section (30) exemptions may be granted provided any personal data is processed:
 - (a) for personal, family or household affairs, including any recreational purposes;

- (b) the enforcement of any legal right or claim;
- (c) the enforcement of any decree of court, tribunal, or for the performance of a judicial or quasi-judicial function;
- (d) for the prevention, detection, investigation, or prosecution of any criminal offence,
- (e) the assessment or collection of any tax or duty or any other imposition of a similar nature by the relevant authority shall be exempted from sections (6), (7), (8) and subsection (2c) of section 9 of this Act and such other related provisions of this Act as may be prescribed under the Rules and Commission for specific purposes permitted under this Act;

2) for the information concerning health services or emergency services of a data principal shall be exempted from subsection (2) of section 9 and other related provisions of this Act;

- (a) for preparing statistics or carrying out research shall be exempted from sections (6), (7), (8) and subsection (2) of section 9 of the Act and other related provisions of this Act, provided that such personal data is not processed for any other purpose and the resulting statistics, or the results of the research shall not be made available in a form that identifies the data principal;
- (b) for discharging regulatory functions shall be exempted from sections (6), (7), (8) and subsection (2) of section 9 patchwork of global and regional if the application of those provisions to the personal data may hamper the proper discharge of those functions;
or
- (c) for journalistic, literary, or artistic purposes shall be exempted from sections (6), (7), (8), (9), (10), (11), (12) and other related provisions of this Act provided that—
 - i. the processing is undertaken for publication;
 - ii. the data fiduciary subject to reasonable grounds of freedom of expression believes that the publication is in the public interest; and
 - iii. the processing is on the grounds of necessity or national security interests of Pakistan.

33. REPEATED COLLECTION OF PERSONAL DATA.—

1) Where a data fiduciary—

- a) has complied with the requirements of this Act concerning the collection of personal data from the data principal, referred to as the “first collection”, and on any subsequent occasion again requests to collect personal data from the same data principal, referred to as the “subsequent collection”, the data fiduciary shall not be required to comply with the requirements of section 7 in respect of the subsequent collection if—
 - i. to comply with those provisions in respect of that subsequent collection would be to repeat, in the same circumstances, what was done to comply with that principle in respect of the first collection; and
 - ii. not more than twelve months have elapsed between the first collection and the subsequent collection.

To avoid ambiguity for this Act, it is asserted that subsection (1) shall not be exercised to prevent a subsequent collection from becoming the first collection if the concerned data fiduciary has complied with the provisions of the notice and consent concerning the subsequent collection.

CHAPTER VII

THE COMMISSION

34. ESTABLISHMENT OF THE COMMISSION.—

- (1) The Federal Government shall, by notification, establish a Commission for this Act which shall be called the National Commission for Personal Data Protection (NCPDP) of Pakistan.
- (2) The Commission shall be an autonomous body under the administrative control of the Federal government with its headquarters located in Islamabad.
- (3) The Commission may set up its establishments including sub-offices at Provincial capitals and such other places, as it may deem necessary from time to time.

(4) The Commission shall be a statutory corporate body, having perpetual succession and a common seal, subject to the provisions of this Act, and shall have the following powers:

(a) The Commission-

- (i) may sue or be sued or enter into contracts;
- (ii) has the power to acquire, purchase, hold, and dispose of both moveable and immovable property;
- (iii) may convey, assign, surrender, charge, mortgage, reassign, transfer or otherwise dispose of or deal with any moveable or immovable property;
- (iv) shall enjoy operational and administrative autonomy, except as specifically provided for under this Act.

35. COMPOSITION AND QUALIFICATION OF MEMBERS OF THE COMMISSION.—

- (1) The Commission shall consist of a Chairman and four other full-time Members, who shall be appointed on the recommendation of the Federal Government.
- (2) The Members appointed under subsection (1) shall choose a Chairman among themselves.
- (3) The Members of the Commission shall be appointed for a term of four years and shall be eligible for re-appointment for a similar term.
- (4) The Members of the Commission shall be public servants within the meaning of section 21 of the Pakistan Penal Code (Act XLV of 1860).
- (5) In the appointment of the Chairman and Members of the Commission, the Federal Government must ensure that the persons shall have the required ability, integrity, and standing to fulfil the functions as prescribed by this Act, and must possess the required qualification, specialised knowledge, and relevant experience in any of the following fields to be eligible for becoming a Member of the Commission, one of whom shall be:
 - (a) ICT expert in the data protection field,
 - (b) a legal expert,
 - (c) strategic interest expert,
 - (d) a representative of civil society; and
 - (e) a financial/accounting expert

36. POWERS OF THE FEDERAL GOVERNMENT TO ISSUE POLICY

DIRECTIVES.—

- (1) The Federal Government may increase the number of Members of the Commission and shall reserve the right to prescribe their qualifications and mode of appointment from time to time, as it considers necessary for effectively dispensing the functions enumerated in this Act.
- (2) The Federal Government may, as and when required, shall issue policy directives to the Commission, not inconsistent with the provisions of this Act, on the matters concerning Personal Data Protection and for matters connected therewith and ancillary thereto, mandates the Commission to comply with such directives.

37. SPECIAL PROVISIONS CONCERNING MEMBERS.—

- (1) The Members of the Commission shall be entitled to a salary and privileges of an officer on the PM-I scale. The Member of the Commission shall not hold any other office of profit including any other public office or relate to any political party or have any conflict of interest concerning this Act while discharging his duties in the Commission as enshrined in the Act.
- (2) A Member of the Commission may resign by giving a written notice thereof to the Federal Government or may be removed from his office by the Federal Government on an inquiry conducted by the Federal Public Service Commission (FPSC) or if found unable to perform the functions of his office because of a mental or physical disability or misconduct or any misappropriation.
- (3) In case of death, resignation, or removal of a member of the Commission, another person may be appointed as such member for the term specified under sub-section (3).

38. APPOINTMENT AND MATTERS OF EMPLOYEES OF THE COMMISSION.—

- (1) The Chairman of the Commission is vested with the powers to decide matters concerning the administration and appointment of new employees by regulations made by the

Commission under section (37) and other relevant regulations made by the Commission from time to time.

- (2) For the performance of functions, the Commission may, from time to time, employ such persons and on such terms and conditions as deemed necessary.
- (3) The employees of the Commission shall be public servants within the meaning of section (21) of the Pakistan Penal Code (Act XLV of 1860).
- (4) Without prejudice to the generality of the foregoing powers, the Commission may;
 - (a) appoint and remove its employees, and officers;
 - (b) exercise discipline and control over employees or officers;
 - (c) prescribe any remuneration, salary or allowances and any such terms and conditions of service of such officers, employees, consultants and experts;
 - (b) regulate and manage its internal organisation, set up divisions within the Commission and make appropriate appointments in those divisions; and
 - (c) appoint advisory bodies, consultants, and advisors on contract to advise the Commission concerning its functions or powers.
- (5) The decision of the Commission shall, subject to subsection (10), be taken with the concurrence of most of its members.
- (6) Notwithstanding anything contained in sub-section (10), no act or proceedings of the Commission shall be invalid by reason only of the existence of a vacancy in, or a defect in the constitution of the Commission.

39. FUNCTIONS OF THE COMMISSION.—

- (1) The Commission shall be responsible to protect the interest of the data principal, precluding illegal activities misusing personal data, promote awareness of data protection, and entertain complaints of data principals made under this Act.
- (2) Without prejudice to the generality of the foregoing and other functions under this Act, the Commission shall perform the following functions:
 - a) Receiving and deciding complaints about infringement of personal data protection including violation of any provision of this Act;
 - b) examining various laws, rules, policies, bye-laws, regulations or instructions about the protection of personal data and may suggest amendments to bring the

law in compliance with the provisions of this Act;

- c) taking proactive steps to create public awareness about personal data protection rights and filing complaints against infringement of those rights, as per the provisions of this Act;
- d) engaging, supporting, guiding, facilitating, training and persuading data fiduciaries, and data processors to ensure the protection of personal data, as per the provisions of this Act;
- e) ensuring that decisions of the Commission shall be based on established principles to ensure transparency and accountability;
- f) monitoring and enforcing the application of the provisions of this Act;
- g) taking prompt and appropriate actions in response to a data security breach, as per the provisions of this Act;
- h) monitoring the cross-border transfer of personal data as per provisions of this Act.
- i) 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;
- j) advising the Federal Government and any other statutory authority on measures that must be undertaken to promote the protection of personal data and to ensure consistency of application and enforcement of this Act;
- k) For the compliance of obligations under the Act, the Commission is entitled to seek professional input from private or public entities.

(3) The Commission shall recommend to the Federal Government, Provincial Governments and any other authority steps required for ensuring the consistency and enforcement of Personal Data Protection policies across Pakistan and suggest measures to make Pakistan's data protection laws in compliance with international standards.

(4) The Federal Government may assign any other functions to the Commission from time to time, as it may consider necessary for effectively discharging functions under this Act.

40. POWERS OF THE COMMISSION.—

(1) The Commission shall exercise powers that enable it to effectively perform its functions as specified in section 35.

(2) Without prejudice to the generality of the foregoing power, the Commission shall-

- a) decide the complaint or pass any order and for this purpose, the Commission shall be deemed to be a Civil Court and shall have the same powers as are vested in a such court under the Code of Civil Procedure Code, 1908 [Act No. V of 1908];
- b) formulate, approve and implement policies, procedures and regulations for its internal administration, operations, human resource management, procurements, financial management and partnerships;
- c) formulate a compliance framework for monitoring and enforcement to ensure transparency and accountability, subject to the measures including but not limited to the following:
 - i. Privacy
 - ii. Transparency
 - iii. Security Safeguards
 - iv. Personal Data Breach
 - v. Data Protection Impact Assessment
 - vi. Record Maintenance
 - vii. Data Audits
 - viii. Responsibilities of Data Protection Officer
 - ix. Processing by entities other than Data Fiduciaries
 - x. Classification of Data Fiduciaries
 - xi. Grievance Redressal mechanism
 - xii. Cross-border data sharing
 - xiii. Cross Border Equivalence Mechanism and matters ancillary thereto
- d) Identify big/large data fiduciary/processors, along with other categories, and define special measures for compliance by the provisions of the Act;
- e) Formulate a Registration Framework for data fiduciaries and data processors under the Act;
- f) Take prompt and appropriate action in response to a data security breach as per the

provisions of this Act;

- g) Powers of search and seizure while handling/ dealing with the complaints;
- h) Prescribe a schedule of costs and the mode of payment, along with its format for filing the complaint;
- i) Seek information from data fiduciary concerning data processing under this Act and impose penalties for non-observance of data security practices and for not complying with the provisions of this Act;
- j) Order a data fiduciary to take such reasonable measures as it may deem necessary to redress the grievances of an applicant in case of non-implementation of the provisions of this Act; and
- k) Summon and enforce the attendance of witnesses to ensure their oral and written evidence under the oath.

41. POWER OF THE COMMISSION TO CALL FOR INFORMATION.—

- (1) Without prejudice to the other provisions of this Act, the Commission may require a data fiduciary or the data processor to provide such information as may be reasonably required by it for the effective discharging of its functions under this Act.
- (2) Whenever the Commission require any information from the data fiduciary or data processor under sub-section (1), the concerned officer of the Commission shall provide a written notice to the data fiduciary or the data processor stating the reason for such requisition in a specified manner and form in which such information may be provided.

42. MEETINGS OF THE COMMISSION.—

- (1) The Chairman and Members of the Commission shall convene in pursuance of the transaction of business, including a quorum constituting at least three members of the Commission for a meeting.
- (2) If for any reason, the Chairman is not available to attend a meeting, the majority of the Members present shall nominate a Member to chair a meeting of the Commission.
- (3) All issues presented before the Commission shall be decided by a majority of votes of the Members present, and in the case where there is an equality of votes, the Chairman, or any member presiding on his behalf shall have the right to casting vote.

- (4) If any member may have a conflict of interest in any matter presented before the Commission, the member shall disclose the nature of the interest at such meeting, which shall be officially recorded by the Commission, and such member shall be barred from taking a part in any meeting or decision concerning that matter.

43. SUBMISSION OF YEARLY REPORTS, AND ANY OTHER INFORMATION.—

- (1) At the end of every financial year but before the end of the next September, the Commission shall submit a report to the Federal Government on the conduct of its affairs, including actions taken for the Personal Data Protection and protection of interest of the data principal for that year.
- (2) A copy of the report specified in sub-section (1) together with a copy of the audit report shall be placed before the National Assembly within three months of the finalisation of the audit report by the Auditor-General.
- (3) The Federal Government may require the Commission to provide any statements, statistics, a copy of any document or any other information concerning any matter under the direct control of the Commission.

44. FUNDS OF THE COMMISSION.—

- (1) There shall be a fund to be known as the "Personal Data Protection Fund" to bear the expenses of the Commission and shall be utilized by the Commission concerning its functions under this Act.
- (2) The bank account of the Personal Data Protection Fund shall be maintained with the National Bank of Pakistan or with any other scheduled bank as the Commission may decide from time to time.
- (3) The Personal Data Protection Fund shall be financed from the following sources, namely:
- (a) Loans and grants from the Federal Government and the Provincial Governments, including an initial grant of XXXXXX million rupees by the Federal Government;
 - (b) Foreign aid, grants and loans negotiated and raised, or otherwise obtained by the Commission with the approval of the Federal Government.

- (c) Fees / Registration Fee and other amounts received by the Commission from time to time.
- (d) Income from the sale of moveable or immoveable property;
- (e) Income from investments; and
- (f) All other sums received or earned by the Commission.

45. MAINTENANCE OF ACCOUNTS AND AUDIT.—

- (1) The accounts of the Commission shall be maintained in such form and such manner as the Federal Government may determine in consultation with the Auditor-General of Pakistan.
- (2) The accounts of the Commission shall be audited at the end of each financial year by the Auditor-General of Pakistan.
- (3) The Commission shall produce such accounts, books, and documents and provide explanations and information as the Auditor-General or any other officer authorised by him on his behalf may require for audit purposes.
- (4) Copies of the Auditor-General's report on the accounts shall be provided to the Commission and the Federal Government and shall also be available for public inspection on the website of the Commission.
- (5) The Commission may, in addition to the audit under sub-section (1), may require its accounts to be audited by any external auditor.

46. CO-OPERATION WITH INTERNATIONAL ORGANIZATIONS.— The commission may, subject to the prior approval of the federal government, shall cooperate with any foreign authority or international organization in the field of data protection/data security/data theft / unlawful data transfer on the terms and conditions of any program or agreement for co-operation to which such authority or organization is a party, or under any other international agreement after the commencement of this act.

CHAPTER VIII

COMPLAINT AND OFFENCES

47. UNLAWFUL PROCESSING OF PERSONAL DATA.—

- (1) Where a data fiduciary or a data processor process, disseminates or discloses any personal data in violation of any of the provisions of this Act shall be punished with fine up to fifteen hundred million rupees and in case of subsequent unlawful processing of personal data, the fine may be raised to twenty-five hundred million rupees.
- (2) In case, where the offence is committed under sub-section (1) and relates to sensitive data the offender may be punished with a fine of up to five thousand million rupees or up to 2% of its total global turnover of the preceding fiscal year, whichever is a higher penalty, shall be assessed by the Commission.

Explanation: For the purpose of this section, “total global turnover” means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement of a data fiduciary where such revenue is generated within Pakistan and outside Pakistan.

48. FAILURE TO ADOPT APPROPRIATE DATA SECURITY MEASURES.—

- (1) Where a data fiduciary or a data processor fails to take adequate security measures to prevent a data breach, as per the provisions laid down in this Act shall be punished with a fine of up to twenty-five hundred million rupees.

49. ISSUE ENFORCEMENT ORDERS AND IMPOSE PENALTIES.—

- (1) Where a data fiduciary or a data processor fails to comply with the orders of the Commission

or the court when required to do so, shall be punished with a fine of up to five hundred million rupees.

- (2) Where a data fiduciary or data processor contravenes any provision of this Act or the rules or regulations made thereunder or policy issued by the Federal Government, or any direction issued by the Commission or condition of the registration, the Commission may by written notice require data fiduciary or data processor within fifteen days as to why an enforcement order may not be issued.
- (3) The notice referred to in sub-section (1) shall specify the nature of the contravention and the steps to be taken by the licensee to remedy the contravention.
- (4) Where anyone fails to: -
 - (a) respond to the notice referred to in subsection (1);
 - (b) satisfy the Commission about the alleged contravention; or
 - (c) provide redressal in writing and providing satisfactory reasons for the contravention within the time allowed by the Commission, shall be-
 - (i) Levied with a fine which may extend to five hundred million rupees;
 - (ii) Faced with a suspension or termination of the registration and shall be imposed with stringent conditions.

50. COMPLAINT.—

- (1) Any person or a concerned data principal shall file a complaint before the Commission against any violation of personal data protection rights, misconduct of any data fiduciary, or data processor as prescribed under this Act involving: -
 - (a) a breach of the data principal's consent to process data;
 - (b) a breach of obligations of the data fiduciary or the data processor in the performance of their functions under this Act;
 - (c) provision of incomplete, misleading, or false information while taking consent of the data principal; or
 - (d) any other matter relating to the protection of personal data.
- (2) The complainant may file a complaint on plain paper or as per a sample format prescribed by the Commission and the complainant shall certify that he had not already or concurrently filed any application, complaint or suit before any other forum or court.

- (3) The Commission shall charge a reasonable fee for filing or processing of the complaint, as prescribed under this Act, and shall also facilitate online receipt of complaints.
- (4) The Commission shall acknowledge the receipt of the complaint within three working days and shall dispose of the complaint by apprising the complainant within thirty days of its receipt or for reasons to be recorded in writing, within such extended time as reasonably determined by the Commission.
- (5) After receipt of the complaint, the Commission may-
 - (a) seek an explanation from the data fiduciary or data processor, after conducting an initial evaluation against whom the complaint has been made by providing him with a reasonable time and opportunity to be heard through an efficient mode of communication; and
 - (b) Contact the complainant, if deemed necessary to seek further information or his comments on the response of the data fiduciary or the data processor, or any other concerned agency.
- (6) The Commission shall efficiently dispose of a complaint and may issue directives to prevent the breach of data protection rights without first seeking comments from the concerned data processor and data fiduciary.
- (7) The Commission may employ electronic means of communication to dispose of complaints and shall maintain an appropriate record of such communications. The Commission shall, as soon as possible establish an online facility to receive, process, manage and dispose of complaints efficiently and cost-effectively.
- (8) Where the data fiduciary or data processor fails to respond to the Commission or execute its orders, the Commission may initiate enforcement proceedings as per rules prescribed under this Act.

51. APPEAL.—

- (1) Appeals against the decisions of the Commission shall be referred to the High Court or to any other Tribunal established by the Federal Government for this Act, in the manner prescribed by the High Court for filing the first appeal before that Court or the Tribunal and the Court or the Tribunal shall decide such appeal within ninety days.

(2) A person aggrieved by any decision or order of any officer of the Commission may, within thirty days of the receipt of the decision or order, shall appeal to the Commission in a prescribed manner and the Commission shall decide such appeal within thirty days.

CHAPTER IX

MISCELLANEOUS

52. TEMPORARY PROVISIONS.— All data fiduciaries and data processors shall adopt necessary security measures within [six months] from the day on which this act comes into force.

53. POWER TO MAKE RULES.—

- (1) The Commission may with the approval of the Federal Government, by notification in the official Gazette, make rules to carry out the purposes of this Act.
- (2) Without prejudice to the generality of the foregoing, these rules may empower the Federal Government to:-
 - a) prepare and encourage the drawing up of suitable codes of conduct and ethics by data processors and data fiduciaries;
 - b) verify the compliance of such codes with applicable laws;
 - c) seek views of the data fiduciaries and data processors in any manner related to electronic data;
 - d) contribute to the publicity and enforcement of such codes;
 - e) interact and cooperate with international and regional bodies performing similar functions; and
 - f) set up or accredit bodies to audit the security measures of the data fiduciaries and data processors.
- (3) All public and regulatory authorities especially in the banking, insurance, telecommunication, legal and health sector shall assist the Commission in the exercise and performance of its powers and functions under this Act.

54. POWER TO MAKE REGULATIONS.—The commission shall issue regulations for exercising its powers and performance of its functions, for its internal working, appointment, promotion, termination and terms and conditions of its employees not inconsistent with the provisions of the act or the rules, for carrying out its functions under this act.

55. RELATIONSHIP OF THE ACT WITH OTHER LAWS.—The provisions of this act shall have effect notwithstanding anything to the contrary contained in any other law on the subject for the time being in force. the articles of this act will serve as bare minimum provisions; wherever there is any other applicable law on the subject, the provisions that have stringent effect will prevail.

56. REMOVAL OF DIFFICULTIES.—If any difficulty arises in giving effect to the provisions of this act, the federal government may, within two years of the commencement of this act and by order published in the official gazette, make such provisions not inconsistent with the provisions of the act as may appear to be necessary for removing the difficulty.

57. WINDING UP OF THE COMMISSION.—No provision of any law relating to the winding up of bodies corporate shall apply to the commission. the commission shall only be wound up by the law to be enacted by the parliament for winding up of the commission.

STATEMENT OF OBJECTS AND REASONS

The right to privacy enshrined in the Constitution of Pakistan is a fundamental right of a person. It emanates that every citizen has a right to the protection of personal data which is an indispensable aspect of informational privacy.

This Bill is to lay out the modus operandi and ancillary details of digital personal data such as collection, storage, disclosure, and its usage by government, organizations, and individuals for processing purposes. It nourishes the environment of a free and fair digital economy by offering legal protections in online transactions and sharing of personal and sensitive information or data for personal, international e-commerce, and e-government services.

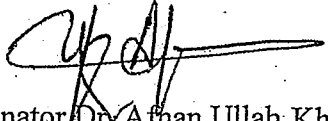
Keeping in view potential approaches, the Personal Data Protection Bill, 2022 is enacted in line with a present patchwork of global, and regional legislations on the protection of personal data to match common grounds and identify areas where different approaches tend to diverge. Rapid technological advancement and enhanced use of internet services have digitised a wide range of economic, political, and social activities that are having a transformational impact on the way businesses were conducted, and the interaction of people amongst themselves, as well as with the government, enterprises, and other stakeholders.

As early adopters of emerging technologies children are also affected by the risks of the digital world, given their developmental vulnerabilities as they are “canaries in the coal mine for threats to us all.” Therefore, the Data Protection Bill, 2022 ensures to afford extra protection for children, concerning their personal and sensitive data. Hailed as amongst the most progressive country on transgender rights globally, Pakistan endeavours to afford extra protection to the personal data of transgender and inter-sex persons. Hence, expressions of gender identity are included in Data Protection Bill, 2022.

Fostering trust online is a fundamental challenge to ensure that the opportunities emerging out of the economy can be fully leveraged. As the global economy shifts to connected information space, its central component is personal data that drives online cross-border commercial activity, the flow of which may affect individuals, businesses, and government.

This Bill ensures that any personal data shall be collected only by lawful and fair means from an individual and must be used or disclosed for the purposes for which the data were collected or any other directly related purpose unless the data principal consents.

Member Incharge



Senator, Dr. Afhan Ullah Khan