Vol: 19523

MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION

DRAFT OF THE PERSONAL DATA PROTECTION BILL, 2023

TABLE OF CONTENTS

STATEMENT OF OBJECTIVES

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 for the usage of personal data such as processing, collection, storage, and disclosure by government, organisations, and individuals for processing purposes because of necessary care, and obligations enunciated in this Bill. It nourishes the environment of fair practices in the 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, of 2023 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, of 2023 ensures to afford extra protection for children, concerning their data.

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, fair, and consensual 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.

PERSONAL DATA PROTECTION BILL, 2023

The Personal Data Protection Bill, 2023 is devised to regulate the collection, processing, use, disclosure, and transfer of personal data and additionally provides a data protection mechanism including the offences concerning the violation of data privacy rights of an individual.

Where a person collects, processes, stores, uses, and discloses data, it must respect the rights, freedoms, and dignity of an individual for matters connected therewith and ancillary thereto. Therefore, the Bill is enacted as follows:

CHAPTER I
PRELIMINARY

(1) Short title, extent, and commencement. – (1) This Act may be called the Personal Data Protection Act, 2023.

(2) It extends to the whole of Pakistan.

(3) It shall come into force not beyond two years from the date of its promulgation as the Federal Government may determine by notifying in the Official Gazette by providing at least three months' advance notice from the effective date.

2. Definitions. – In this Act, unless there is anything repugnant in the subject or context, ——

(a) **"anonymized data"** means 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;

(b) "**authorised person**" means a person or a guardian authorised by the court to make a data access or data correction request;

(c) **"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 dactyloscopic data;

(d) **"child"** means a person who has not attained the age of eighteen years;

(e) **"Commission"** means the National Commission for Personal Data Protection (NCPDP) of Pakistan established under section 35 of the Act;

(f) **"consent"** means any freely given, specific, informed, and unambiguous indication of the data subject's intention by which the data subject by a statement or by clear affirmative action, signifies agreement to the collecting, obtaining, and processing of personal data provided that it conforms with section 13 and 14 of the Contract Act, 1872;

(g) **"critical personal data"** means such personal data retained by the public service provider - excluding data open to the public - as well as data identified by sector regulators and classified by the Commission as critical or any data related to international obligations;

(h) **"data controller"** means a person or the government, who either alone or jointly has the authority to decide on the collection, obtaining, usage, or disclosure of personal data;

(i) **"data processor"** means a person or the government who alone or in conjunction with other(s) processes data on behalf of the data controller;

(j) **"data subject"** means a natural person who is the subject of the personal data;

(k) "**disability"** means the inability to engage in any substantial gainful activity because of any medically determinable physical or mental impairment or is perceived to exist whether or not it exists, 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;

(l) **"financial data"** means information regarding finances, including, but not limited to assets, income, liabilities, net worth, bank balances, financial history, any specific information of financial nature or any financial activities, or credit history;

(m) **"foreign data subject"** means a data subject who is not a Pakistani national;

(n) **"genetic data"** means personal data relating to 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 results in particular, from an analysis of a biological sample from the natural person in question;

(o) **"Government"** means the Federal Government, Provincial Government, and Local Governments and divisions or entities under their control;

(p) **"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 extortion, under the circumstances, or withdrawal of any services and benefit due to an evaluative decision about data subject;

(q) **"health data"** means any personal data related to the physical or mental health of a data subject including the recordings regarding the past, present, or future state or provision of health care services, which may reveal information about his health status;

(r) **"healthcare professional"** means a medical practitioner, dental practitioner, pharmacist, clinical psychologist, nurse, midwife, medical assistant, physiotherapist, occupational therapist, and other allied healthcare professionals and any other person involved in giving medical, health, dental, pharmaceutical or any other healthcare services authorised to provide such services under the laws of Pakistan;

(s) **"international obligations"** means the same as defined under Part 1 of the Fourth Schedule of the Constitution of the Islamic Republic of Pakistan, 1973;

(t) **"journalistic purpose"** means any activity intended towards the dissemination through print, electronic, or any other media that includes factual reports, analysis, opinions, views, or documentaries news regarding recent or current events;

(u) **"legitimate interest"** means anything permitted under the law;

(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) **"medical purposes"** includes the purposes of preventive medicine, medical diagnosis, medical research, rehabilitation and the provision of care and treatment, and the management of healthcare services;

(x) "**parental consent"** includes the consent of a lawful guardian, where applicable;

(y) **"person"** includes:

(i) an individual;
(ii) a company;
(iii) a firm;
(iv) or an association or body of individuals, whether incorporated or not;

(z) **"personal data"** means any information that relates directly or indirectly to a data subject, who is identified or identifiable 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;

(aa) **"personal data breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(bb) **"prescribed"** means as prescribed by Rules made under the provisions of this Act;

(cc) **"processing"** means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(dd) **"profiling"** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to the data subject in particular to analyse or predict aspects concerning that data subject's attributes related to employment, social preferences, religious beliefs, economic situation, health, reliability, behaviour, location or movements;

(ee) **"pseudonymisation"** means 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(ff) **"public interest"** means any matter about the general welfare of the public that warrants recognition and protection; and subject in which the public as a whole has a stake; especially an interest or common interest in conformity with laws of the land;

(gg) **"public service provider"** means and includes any entity dealing with and having personal data while working under government;

(hh) **"relevant person"** means a data subject:

(i) in the case of an individual who has not attained the age of eighteen years, therefore, his parent or a guardian appointed by a court of competent jurisdiction shall manage his affairs;

(ii) who is incapable of managing his affairs, therefore, a person appointed by a court may serve on his behalf to run his affairs; or

(iii) who is authorised by the data subject to make a request for data access and/or data correction;

(ii) **"requestor"** means anybody who makes a request under this Act for any matter related or ancillary thereto this Act;

(jj) **"Rules"** means rules made under sec 54 of this Act;

(kk) "**Sensitive personal data**" means any personal data relating to:

(i) financial information excluding identification number, credit card data, debit card data, account number, or other payment instruments data;

(ii) health data (physical, behavioural, psychological, and mental health conditions, or medical records);

(iii) computerized national identity card or passport;

(iv) biometric data;

(v) genetic data;

(vi) religious beliefs;

(vii) criminal records;

(viii) political affiliations;

(ix) caste or tribe;

(x) individual's ethnicity;

(ll) **"Significant"** means any data controller or processor which is sufficiently great or important to be worthy of attention by its sales revenue, profit, number of employees, market share, capital employed, or any other indicator such as number of users, type of data collected or a combination thereof that may constitute it as significant;

(mm)**" The State"** means the same as defined under Article 7 of the Constitution of the Islamic Republic of Pakistan, 1973;

(nn) **"third party** "means any person other than—

(i) a data subject;
(ii) a relevant person concerning a data subject;
(iii) a data controller;
(iv) a data processor; or
(v) a person under the direct control of the data controller, who is authorised in writing to process the personal data;

(oo) **"vital interests"** means matters relating to life, fundamental rights, security of data subject to humanitarian emergencies, in particular in situations of natural and man-made disasters, and monitoring and management of epidemics.

3. Scope and applicability. –

This Act shall apply–

(a) Where any data controller or a data processor processes or exercises control or authorises the processing of any personal data, provided that they shall be established/present/registered within the territory of Pakistan.

(b) Where any data controller or a data processor whether digitally or non-digitally operational within Pakistan but incorporated in any other jurisdiction, carries out processing of personal data concerning any commercial or non-commercial activity including profiling data subjects within the territory of Pakistan.

(c) Where a data controller and a data processor not having a physical presence within the territory of Pakistan carries out the processing of personal data in a territory where Pakistani law applies under public or private international law.

(d) Where a data controller or data processor collects personal data of a data subject within the territory of Pakistan including a foreign data subject who is physically present at the time of collection, and processing of personal data within the territory of Pakistan.

Provided that in the case of the foreign data subject, the collection is not in conflict with the privacy laws of the country where the data controller is registered.

4. Interpretation. –

In this Act, unless the context otherwise requires, the following terms shall be read about Rules made under this Act, and the pronouns "he" and "his" have been used throughout this Act for an individual, irrespective of gender.

CHAPTER II
PROCESSING OF PERSONAL DATA AND OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

5. Grounds for processing personal data. –

(1) Personal data shall be collected, processed, and disclosed by a data controller/data processor lawfully and fairly by complying with the provisions of this Act.

(2) The personal data shall be collected for specified, explicit and legitimate purposes, which shall not be processed further that is incompatible with the aforementioned purposes and shall be adequate, relevant, and limited to the purposes for which the data is processed.

(3) The data controller and/or data processor whether digitally or non-digitally operational within the territory of Pakistan shall register with the Commission in such manner as may be specified by the registration framework to be formulated by the Commission provided that the data controller and/or data processor is already registered with any public body in that case, it shall only be required to intimate the Commission.

(4) The data controller and/or data processor identified as "significant" by the

Commission shall be required to appoint a data protection officer, who is well-versed in the collection and processing of personal data and the risks associated with processing.

6. Consent for personal data processing. -

(1) The personal data of any kind of a data subject shall not be processed unless the data controller seeks his consent before the commencement of the processing of the data or as prescribed under the provisions of this Act.

(2) The consent of the data subject under sub-section (1) must be a free, specific, informed, and unambiguous indication of the data subject's intentions 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 subject has given his consent to the processing of data under this section shall lie with the data controller.

(4) The data subject 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 a data subject. 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 subject withdraws his consent to the processing of personal data under-sub-section (4), the data controller shall, within a reasonable time, cease and direct its data processors to cease processing the personal data of such data subject unless such processing can happen without the consent of data subject or authorised under the law.

(6) Notwithstanding sub-section (1), a data controller may process the personal data of a data subject if the processing is necessary for the following: -

(a) for the performance of a contract to which the data subject is a party;

(b) for taking steps at the request of the data subject to enter into a contract;

(c) for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;

(d) 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 subject or any other individual;

(e) for protecting the vital interests of the data subject;

(f) for compliance with any court order of competent jurisdiction;

(g) for legitimate interests pursued by the data controller; or

(h) for the exercise of any functions conferred on any person by or under any law.

7. Notice to the data subject. –

(1) A data controller shall by written notice including digitally inform a data subject or where this is not practical, it shall be provided by another data controller that exercises control over the same personal data—

(a) that is collected by or on behalf of a data controller, along with its description;

(b) to provide the legal basis for the processing of personal data and the time duration for which data is likely to be processed and retained thereafter for the purpose for which the personal data is or to be collected and processed further;

(c) of any information available to the data controller as to the source of that personal data;

(d) information regarding any cross-border transfer of personal data that the data controller intends to carry out, if applicable;

(e) inform the data subject about their rights as mentioned in this Act including the data subject's right to request access and correction of the personal data and provide information on contacting the data controller with any inquiries or complaints concerning personal data;

(f) provide the list of third parties to whom the data controller shall or may disclose the personal data;

(g) the choices and means, the data controller offer the data subject for restricting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;

(h) whether it is obligatory or voluntary for the data subject to supply the personal data; and

(i) where it is obligatory for the data subject to supply the personal data, but in case of failure to comply with the request, the data subject shall face the consequences.

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

(a) when the data controller first requests the data subject to provide his personal data;

(b) when the data controller first collects the personal data of the data subject; or

(c) in any other case, before the data controller—

(i) uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or

(ii) discloses personal data to a third party.

(3) A notice under sub-section (1) shall be served in English or any other language as specified in Article 251 of the Constitution of the Islamic Republic of Pakistan, 1973; and the individual shall be provided with a clear and readily accessible means to choose his choice of language.

8. Non-disclosure of personal data. –

Subject to section 24, personal data without the consent of the data subject shall not be disclosed—For any purpose other than—

(a) the one for which the personal data was to be disclosed at the time of collection of the personal data; or

(b) a purpose directly related to the purpose referred to in clause (a) of sub-section (1); or

(c) to any party other than a third party as specified in clause (f) of sub-section (1) of section 7.

9. Security requirements. –

(1) Given the national interest, the Commission shall prescribe the best international standards to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration, or destruction.

(2) A data controller or processor shall when collecting or processing personal data must take practical measures to protect the personal data as per the terms mentioned herein below by considering the nature of the personal data and the harm that may result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration, or destruction:

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

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

(5) Save as other related laws will also remain in the field of their respective domains.

10. Data retention requirements. –

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

(2) It shall be the duty of a data controller 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 sub-section (1).

11. Data integrity. -

A data controller shall take adequate steps to ensure that the required personal data is accurate, complete, not misleading, and kept up to date concerning any direct or indirect purpose for which the personal data was collected and processed further.

12. Record to be kept by the data controller. –

(1) A data controller shall keep and maintain a record of each application, notice, request, or any other information concerning the personal data that has been or is processed by him.

(2) The Commission may determine the manner and form in which the record is to be maintained.

(3) The data controller shall apprise the Commission regularly about the type of data they are collecting, and the processing undertaken on the collective data, as required under

this Act. 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 subject, as enshrined in the Constitution of the Islamic Republic of Pakistan, 1973.

13. Personal data breach notification. –

(1) In the event of a personal data breach, the data controller shall without undue delay and where reasonably possible, not beyond 72 hours of becoming aware of the personal data breach, must notify the Commission and the data subject except where the breach is unlikely to result in the infringement of rights and freedoms of the data subject.

(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 subject with a valid reason for the delay.

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

(4) The data controller 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 except that the data processor should only inform the data controller and commission.

CHAPTER III

PROCESSING CHILDREN'S PERSONAL DATA

14. Processing personal data of children. –

(1) Every data controller or data processor shall process a child's personal data in such a manner that protects the rights and interests of a child.

(2) The data controller or a data processor shall, before processing any personal data relating to a child, verify his age and seek the consent of his parent or relevant person or authorised 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 controller or a data processor shall not process any personal data of a child that is likely to cause him harm.

(5) A data controller or a data processor 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.

CHAPTER IV

ADDITIONAL REQUIREMENTS FOR PROCESSING SENSITIVE AND CRITICAL PERSONAL DATA

15. Processing of sensitive and critical personal data. –

(1) Subject to sub-section (6) of section 6, a data controller shall not process any sensitive and critical personal data of a data subject except under the following conditions:

(a) the data subject has given his explicit consent to the processing of the personal

data provided that this consent is not restricted by any other applicable law, and any of the following:

(i) for exercising or defending any right or obligation which is conferred or imposed by law on the data controller in connection with employment; or

(ii) to protect the vital interests of the data subject or another person, in a case where—

(a) consent cannot be given by or on behalf of the data subject; or

(b) the data controller cannot reasonably be expected to obtain the consent of the data subject;

(iii) to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;

(iv) for medical purposes which are undertaken by—

(a) a healthcare professional; or

(b) a person who in the circumstances owes a duty of confidentiality which may arise and shall be equivalent as if that person was a healthcare professional;

(v) for, or in connection with, any legal proceedings;

(vi) for obtaining legal advice while ensuring its integrity and secrecy;

(vii) for establishing, exercising, or defending legal rights;

(viii) for the administration of justice under orders of a court of competent jurisdiction; or

(ix) for the exercise of any functions conferred on any person by or under any written law;

(b) the information contained in the personal data is made public advertently by the data subject.

(2) The Commission may by order published in the Gazette exclude the application of clauses (i), (viii), or (ix) of clause (b) of sub-section (1) in such cases as may be specified in the order, or provide that, in such cases, as may be specified in the order, any condition mentioned in the aforementioned clauses is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

CHAPTER V

RIGHTS OF DATA SUBJECTS

16. Right, to access. –

(1) A data subject shall be given access to his personal data held by a data controller except where compliance with a request to access is declined under the provisions of this Act.

(2) A data subject shall have the right to obtain confirmation from a data controller whether the personal data of a data subject is under processing or has been processed, by or on behalf of the data controller.

(3) A requestor may upon payment of a prescribed fee based on an administrative cost, make a data access request in writing to the data controller: -

(a) for information regarding the data subject's personal data that is being processed by or on behalf of the data controller; and

(b) to provide him with a copy of the personal data in an intelligible form.

(4) Where a data controller has shared the data with another data controller/processor, therefore, the first data controller possessing any consent of the data subject shall be liable as provided under sub-section (3).

17. Compliance with the data access request. –

(1) Subject to sub-section (2) of section 31 a data controller shall comply with a data access request under section 16 not later than thirty days from the date of receipt of the data access request.

(2) A data controller who is unable to comply with a data access request within the period as specified in sub-section (1) must before the expiration of that period—

(a) By a written notice inform the requestor and the Commission that the data controller is unable to comply with the data access request within such period and shall furnish the reasons for his non-compliance; and

(b) comply with the data access request to the extent possible.

(3) Notwithstanding sub-section (2), the data controller shall entirely comply with the data access request, not later than fourteen days after the expiration of the period as stipulated in sub-section (1).

18. Circumstances of refusal to comply with the data access request. –

(1) A data controller may refuse to comply with a data access request under section 16 if—

(a) the data controller is not supplied with such information as the data controller may reasonably require—

(i) to satisfy itself concerning the identity of the requestor; or

(ii) where the requestor claims to be a relevant person to satisfy itself—

(a) as to the identity of the data subject concerning whom the requestor claims to be the relevant person; and

(b) that the requestor is the relevant person in relation to the data subject;

(iii) to locate the personal data to which the data access request relates;

(b) the data controller cannot comply with the data access request without disclosing personal data relating to another individual who can be identified from that information, unless—

(i) another individual has consented to the disclosure of the information to the requestor; or

(ii) it is reasonable in all the circumstances to comply with the data access request without receiving the consent of the other individual;

(c) providing access may constitute a violation of any court order;

(d) providing access may disclose confidential information relating to the business of the data controller; or

(e) such access to personal data is regulated by another law.

(2) In determining for the purposes of clause (ii) of subparagraph (b) of sub-section (1) whether it is reasonable in all the circumstances to comply with the data access request without the consent of the other individual, regard shall be given in particular to—

(a) any duty of confidentiality owed to the other individual;

(b) any steps taken by the data controller to seek the consent of the other individual;

(c) whether the other individual is capable of giving consent; and

(d) any express refusal of consent by the other individual.

(3) Clause (c) of sub-section (1) shall not operate to excuse the data controller from complying with the data access request under sub-section (1) of section 16 to any extent that the data controller can comply with the data access request without contravening the prohibition concerned.

19. Right to correction. –

Where—

(a) a data controller has supplied a copy of the personal data in compliance with the data access request under section 16 after which the requestor considers that the personal data is inaccurate, incomplete, misleading, or not up to date; or

(b) the data subject knows that his personal data held by the data controller is inaccurate, incomplete, misleading, or not up to date, therefore, the requestor or data subject may make a data correction request in writing to the data controller to make the necessary correction.

(c) Where a data controller has shared the data with another data processor or a controller, the data controller possessing the consent of the data subject shall be liable under Section 19.

20. Compliance with a data correction request. –

(1) Subject to sub-sections (2), (3), and (5) and section 19, where a data controller is satisfied that the personal data to which a data correction request relates is inaccurate, incomplete, misleading, or not up to date, he shall, not later than thirty days from the date of receipt of the data correction request—

(a) make the necessary correction to the personal data;

(b) supply the requestor with a copy of the corrected personal data; and

(c) subject to sub-section (4), where—

(i) the personal data has been disclosed to a third party during the twelve months immediately preceding the day on which the correction is made; and

(ii) the data controller has no reason to believe that the third party has ceased to use the personal data for the purpose for which it was disclosed to the third party and therefore, shall take all practicable steps to supply the third party with a copy of the corrected personal data along with a written notice stating the reasons for the correction.

(2) A data controller who is unable to comply with a data correction request within the period specified in sub-section (1) shall before the expiration of that period—

(a) by written notice to inform the requestor and the Commission that he is unable to comply with the data correction request within such period and the reasons for his

non-compliance; and

(b) comply with the data correction request to the extent possible.

(3) Notwithstanding sub-section (2), the data controller shall entirely comply with the data correction request not later than fourteen days after the expiration of the period stipulated in sub-section (1).

(4) A data controller is not required to comply with clause (c) of sub-section (1) in any case where the disclosure of personal data to a third party consists of the third party's inspection of a register—

(a) in which the personal data is entered or otherwise recorded; and

(b) available for public inspection.

(5) Where a data controller is requested to correct personal data under sub-section (1) of section 17 and the personal data is being processed by another data controller that is in a better position to respond to the data correction request—

(a) the first-mentioned data controller shall immediately transfer the data correction request to such data controller, and notify the requestor of this fact; and

(b) sections 17, 18, 19, and 20 shall apply as if the references therein to a data controller were references to such other data controller.

21. Circumstances of refusal to comply with the data correction request. –

(1) A data controller may refuse to comply with a data correction request under section 20 if—

(a) the data controller is not supplied with such information as it may reasonably require—

(i) to satisfy itself as to the identity of the requestor; or

(ii) where the requestor claims to be a relevant person to satisfy himself—

a) as to the identity of the data subject with whom the requestor claims to be the relevant person; and

b) that the requestor is the relevant person to the data subject;

(b) the data controller is not supplied with such information as it may reasonably require ascertaining in what way the personal data to which the data correction request relates is inaccurate, incomplete, misleading, or not up to date;

(c) the data controller is not satisfied that the personal data to which the data correction request relates is inaccurate, incomplete, misleading, or not up to date;

(d) the data controller is not satisfied that the correction which is the subject of the data correction request is accurate, complete, not misleading, or up to date; or

(e) subject to sub-section (2), any other data controller controls the processing of the personal data to which the data correction request relates in such a way as to prohibit the first-mentioned data controller from complying, whether in whole or in part, with the data correction request.

(2) Clause (e) of sub-section (1) shall not operate to excuse the data controller from complying with sub-section (1) of section 20 concerning the data correction request to any extent that the data controller can comply with that sub-section without contravening the prohibition concerned.

22. Notification of refusal to comply with a data correction request. –

(1) Where a data controller in pursuance of section 21 refuses to comply with a data correction request under section 20, it shall not later than thirty days from the date of receipt of the data correction request by written notice inform the requestor and the Commission: -

(a) about the refusal and its reasons; and

(b) where clause (e) of sub-section (1) of section 21 is applicable, it shall provide the name and address of the concerned data controller.

(2) Without prejudice to the generality of sub-section (1), where personal data to which the data correction request relates is an expression of opinion and the data controller is not satisfied that the expression of opinion is inaccurate, incomplete, misleading, or not up to date, the data controller shall—

(a) make a note, whether annexed to the personal data or elsewhere—

(i) about the matters concerning the expression of opinion, which is considered by the requestor to be inaccurate, incomplete, misleading, or not up to date; and

(ii) in a way, where the personal data cannot be used by any person without bringing the note to the attention of and making it available for the inspection of that person; and

(b) attach a copy of the note to the notice referred to in sub-section (1) relating to the data correction request.

(3) In this section, "expression of opinion" includes an assertion of fact that is unverifiable or in all circumstances of the case is not practicable to verify.

23. Right to the withdrawal of consent. –

(1) A data subject may, by a written notice withdraw his consent to the processing of personal data which relates to him at any point in time.

(2) The data controller shall, upon receiving the notice under sub-section (1), 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 controller to comply with sub-section (2) shall be construed as an offence and convicted, therefore, liable to a fine not exceeding 50,000 USD or an amount equivalent to Pakistani Rupees.

24. The extent of disclosure. –

Notwithstanding section 8, the personal data of a data subject may be disclosed by a data controller for any purpose other than the purpose for which the personal data was stated to be disclosed at the time of its collection or any other purpose directly related to that purpose under the following circumstances:

(a) the data subject has given his consent to the disclosure;

(b) the disclosure —

(i) is necessary for preventing or detecting a crime, or for investigations; or

(ii) was required or authorised by or under any law or by the order of a court;

(c) the data controller acted in the reasonable belief that in law he has the right to disclose the personal data to the other person;

(d) the data controller acted in the reasonable belief that he had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or

(e) the disclosure was justified in the interest of the public due to the circumstances determined by the Commission in advance of the disclosure.

25. Right to prevent processing likely to cause damage or distress. –

(1) Subject to sub-section (2), a data subject may, at any time shall issue a notice in writing, including digitally to a data controller referred to as the "data subject notice" require the data controller at the end of such period as its reasonable in the circumstances, to—

(a) cease the processing of or processing for a specified purpose or manner; or

(b) not begin the processing of or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject if, based on reasons to be stated by him—

(i) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or distress to him or a relevant person; and

(ii) the damage or distress is or would be unwarranted.

(2) Sub-section (1) shall not apply where—

(a) the data subject has given his consent;

(b) the processing of personal data is necessary—

(i) for the performance of a contract to which the data subject is a party;

(ii) for taking steps at the request of the data subject to enter a contract;

(iii) for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by contract; or

(iv) to protect the vital interests of the data subject; or

(c) in such other cases as may be prescribed by the Federal Government upon recommendations of the Commission by publishing in the Official Gazette.

(3) The data controller shall, within twenty-one days from the date of receipt of the data subject notice under sub-section (1), give the data subject a written notice including digitally —

(a) stating that he has complied or intends to comply with the data subject notice; or

(b) stating his reasons for regarding the data subject notice as unjustified, or to any extent unjustified, and the extent, if any, to which he has complied or intends to comply with it.

(4) Where the data subject is dissatisfied with the failure of the data controller to comply with the data subject notice, whether in whole or in part, under clause (b) of sub-section (3), the data subject may submit a complaint to the Commission to require the data controller to comply with the data subject notice.

(5) Where the Commission is satisfied that the complaint of the data subject under sub-section (4) is justified or justified to any extent, the Commission may require the data controller to take such steps for complying with the data subject notice

26. Right to erasure. –

(1) The data subject shall have the right to request the data controller to erase his personal data concerning him without undue delay and the data controller shall have the obligation to erase personal data within 14 days where one or more of the following conditions applies:

(a) the personal data is no longer necessary concerning the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based under sub-section (1) of section 23 and where there is no other legal ground for the processing; or

(c) the data subject objects to the processing under sub-section (2) of section 23;

(d) the personal data have been unlawfully processed; or

(e) the personal data must be erased for compliance with a legal obligation.

(2) Where the data controller has made the personal data public and is obliged under sub-section (1) to erase the personal data, therefore, the data controller- taking into account of available technology and the cost of implementation- shall take adequate steps, including technical measures to inform data processors processing the personal data for erasure, along any links to, copy or replication of the personal data.

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

(a) for exercising the right of freedom of expression and information as enshrined in the Constitution of the Islamic Republic of Pakistan, 1973;

(b) for compliance with a legal obligation or the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(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 in so far as the right referred to in sub-section (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.

27. Right to nominate. – In the event of the death or disability of the data subject, he shall have the right to nominate, any other individual as may be prescribed, to exercise the rights of the data subject under the provisions of this Act.

28. Right to redressal of grievance. –

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

(2) In the case where a data controller fails to satisfy a data subject 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 data portability and automated processing. –

(1) The data subject shall have the right to receive, his personal data from a data controller in a proper form, that is easy to use and in a machine-readable format, and the data subject shall have the right to transmit that data to another data controller or processor without any objection where:
   (a) the data subject has given his explicit consent; and
   (b) the processing is carried out by automated means.

(2) The data subject shall have the right to transmit his personal data from one data controller to another directly, where it is technically feasible.

(3) Sub-section (1) shall not apply to the extent that processing is necessary for the performance of a task carried out in the public interest.

(4) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which results in legal obligations or significantly harms the data subject, unless the data subject has given his explicit consent.

(5) The data subject shall have the right to obtain from the data controller:
   (a) specific information about automated decision-making including profiling,
   (b) human intervention

(6) The data subject rights mentioned in sub-section (4) shall not apply to the extent where processing is necessary for the performance of a task carried out in the public interest.

(7) The rights mentioned in this section shall not affect the rights and freedoms of other data subjects.

CHAPTER VI
TRANSFER OF PERSONAL DATA OUTSIDE PAKISTAN

30. Restrictions on transferring personal data.- (1) Personal data shall not be transferred to any unauthorised person or system or anything contrary to the provisions of this Act.

31. Condition for Cross border transfer. –

(1) Where personal data excluding critical personal data is required to be transferred to an entity/entities or system located beyond the borders of Pakistan, which is not under the direct control of the Government of Pakistan, it shall be ensured that the country where the data is being transferred offers at least adequate personal data protection legal regime which is consistent to the protection provided under this Act and the data which is transferred shall be processed as per the provisions of this Act and, where applicable, the data subject shall give explicit consent.

(2) Critical Personal Data shall only be processed in a server(s) or digital infrastructure located within the territory of Pakistan.

32. Framework on conditions for cross-border transfer. –

(1) Personal data other than those categorised as critical personal data may be transferred outside the territory of Pakistan after fulfilling necessary explicit consent requirements under this Act. In the absence of an adequate data protection legal regime, the Commission may allow for the transfer of personal data outside Pakistan in the following cases:

(a) Binding contract/agreement;
(b) Explicit consent of the data subject that does not conflict with the public interest or national security of Pakistan;
(c) International cooperation is required under relevant international obligations; and
(d) any further conditions specified by the Commission.

(2) The Commission shall also devise a mechanism for sharing sensitive personal data with the government of Pakistan provided that the data relates to public order or national security and the same is required within the parameters of applicable law. The data controllers or

data processors are also required to share a copy of the requested data in the stipulated timeframe, as prescribed by the Commission.

CHAPTER VII
EXEMPTIONS

33. Repeated collection of personal data–

(1) where a data controller—

(a) has complied with the requirements of this Act concerning the collection of personal data from the data subject, referred to as the "first collection"; and on any subsequent occasion again requests to collect personal data from the same data subject, referred to as the "subsequent collection" the data controller shall not be required to comply with the requirements of section 8 in respect of the subsequent collection if—

(i) to comply with those provisions in respect of that subsequent collection means 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.

(2) It is asserted that sub-section (1) shall not be exercised to prevent a subsequent collection from becoming the first collection if the concerned data controller has complied with the provisions of the notice and consent concerning the subsequent collection.

34. Exemption. –

(1) The personal data processed by an individual only for that individual's personal, family, or household affairs, including recreational purposes, shall be exempted from the provisions of this Act.

(2) Subject to section 15 exemptions may be granted provided personal data is: -

(a) processed for –

(i) the prevention, detection, investigation, or prosecution of any criminal offence;

(ii) the apprehension or prosecution of offenders;

(iii) the enforcement of any legal right or claim;

(iv) the enforcement of any decree of court, tribunal, or for the performance of a

judicial or quasi-judicial function; or

(v) the assessment or collection of any tax or duty or imposition of any levy by the relevant authority shall be exempted from sections 6, 7, 8, and sub-section (2) of section 9 of this Act or as may be prescribed under the Rules and Commission for specific purposes permitted under this Act;

(b) processed concerning information on the physical or mental health of a data subject shall be exempted from sub-section (2) of section 9 and other related provisions of this Act of which the application of the provisions to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other individual;

(c) processed for preparing statistics or carrying out research shall be exempted from sections 6, 7, 8, and sub-section (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 that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;

(d) necessary for or in connection with any order or judgment of a court shall be exempted from sections 6, 7, 8 and sub-section (2) of section 9 of the Act and other related provisions of this Act;

(e) processed to discharge regulatory functions shall be exempted from sections 6, 7, 8 and sub-section (2) of section 9 of the Act and other related provisions of this Act if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions; or

(f) only processed for journalistic, literary, or artistic purposes shall be exempted from sections 6, 7, 8, 9, 10, 11, 12, and sub-section (1) of section 16 and other related provisions of this Act provided that—

(i) the processing is undertaken for publication;

(ii) the data controller subject to a reasonable belief that taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; and

(iii) the processing is on grounds of national security interests of the State provided that the processing of personal data shall not be permitted unless it is authorised pursuant to an express authorisation by the Commission.

(3) Subject to section 33 infrastructure providers whose infrastructure is used by the data

controller and/or data processor and do not process the data may apply for exemptions as permitted under this Act, and Rules made thereunder.

(4) The Commission may propose time-bound exemption to the Federal Government if requested by a data controller or data processor only in case of specific situations/use cases.

CHAPTER VIII
THE COMMISSION

35. Establishment of the Commission. –

(1) The Federal Government shall, by a Gazetted notification, establish a Commission for this Act, which shall be called the National Commission for Personal Data Protection (NCPDP) of Pakistan, within six months of the commencement of this Act.

Provided that the Federal Government may increase the number of members of the Commission and prescribe their qualifications and mode of appointment, as it considers necessary for effectively dispensing the functions enumerated in this Act.

(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 for the purpose of this Act;

(ii) has the power to acquire, purchase, hold, and dispose of both moveable and immovable property of every description;

(iii) may convey, assign, surrender, charge, mortgage, reassign, transfer or otherwise dispose of or deal with any moveable or immovable property or any interest vested in it;

(iv) shall enjoy operational and administrative autonomy, except as specifically provided for under this Act.

36. Composition and qualification of members of the Commission. –

(1) The Commission shall consist of a Chairperson and four other full-time Members, who shall be appointed on the recommendation of the Federal Government.

(2) The Federal Government shall, from amongst the members appointed under sub-section (1), appoint a member to be the Chairperson of the Commission.

(3) The Members of the Commission shall be appointed by the Federal Government for a term of three years and shall be eligible for an extension for a term of two years.

(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 Chairperson 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) an ICT expert with a speciality in cyber security;

(b) a legal expert;

(c) a data policy or privacy expert;

(d) a representative of civil society; and

(e) a financial or business expert.

37. Special provisions concerning members. –

(1) The Members of the Commission shall be entitled to a salary and privileges of an officer on the SPPS scale or equivalent. 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 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) of section 36.

38. Appointment and matters of employees of the Commission. –

(1) The Chairperson of the Commission is vested with the power to decide matters concerning the administration and appointment of new employees by 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;

(d) regulate and manage its internal organisation, set up divisions within the Commission and make appropriate appointments in those divisions; and

(e) appoint advisory bodies, consultants, and advisors on contract to advise the Commission concerning its functions or powers.

(5) The decision of the Commission subject to sub-section (1) shall be taken with the concurrence of the majority of its members.

(6) Notwithstanding anything contained in sub-section (1), no Act or proceedings of the Commission shall be invalid only because 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 subject, enforcing the protection of personal data, precluding illegal activities, and misusing personal data, promoting awareness of data protection, and entertaining complaints of data subjects 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 conformity with the provisions of the 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 controllers, and data processors to ensure the protection of personal data as per the provisions of this Act;

(e) ensuring that all its decisions are based on established principles to structure or minimize discretion and ensure transparency and accountability;

(f) monitoring and enforcing the application of the provisions of this Act;

(g) taking prompt and appropriate action 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, Local Governments, and any entity falling under their domains should take 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 39 and under the provisions of this Act.

(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 is deemed to be a Civil Court and shall have the same powers as are vested in 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 the data controller
(x) Classification of the data controller
(xi) Grievance redressal mechanism
(xii) Special permissions regarding biometric data
(xiii) Cross-border data sharing
(xiv) Adequacy framework for cross-border data flows
(xv) Data portability and automated processing including profiling

(d) Identify other categories including big/large /significant data controllers /processors, and define special measures for compliance by the provisions of the Act or Rules

and regulations;

(e) Formulate a registration framework for data controllers and data processors under the Act or Commission may impose additional requirements under sub-section 3 of Section 5;

(f) Take prompt and appropriate action in response to a data security breach as per the provisions of the Act;

(g) Powers of search and seizure while taking cognizance of the complaint;

(h) Prescribe a schedule of costs and the mode of payment for filing the complaint, its format, and matters ancillary thereto;

(i) Seek information from data controllers 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) Prescribe increased penalties/fines after every three years if deems appropriate;

(k) Order a data controller to take such reasonable measures as it may deem necessary to redress the grievances of an applicant in case of non-implementation of any provision of this Act; and

(l) Summon and enforce the attendance of witnesses and ensure their oral and written evidence under oath;

(m) To take any action to carry out the purposes of this Act.

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 controller or the data processor to provide such information as may be reasonably required by it for effectively discharging its functions under this Act.

(2) Whenever the Commission requires any information from the data controller or data processor under sub-section (1), the concerned officer of the Commission shall provide a written notice to the data controller 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 Chairperson shall chair and convene a meeting of the Commission.

(2) In case, where the position of the Chairperson is vacant or he is not available, the

majority of the Members present can decide, who may convene and chair a meeting of the Commission.

(3) The quorum of the meeting for the Commission shall consist of at least three or five members.

(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. Powers to issue policy directives. – The Federal Government 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.

44. Submission of yearly reports, returns, etc.–

(1) At the end of every financial year but before the last date of the following September, the Commission shall submit a report to the Federal Government through the Prime Minister on the conduct of its affairs, including action taken for personal data protection and protection of interest of the data subjects, 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 finalization of the audit report by the Auditor-General.

(3) The Federal Government may require the Commission to provide any return, statement, estimate, statistics, or other information concerning any matter under the control of the Commission or a copy of any document in the custody of the Commission.

45. Funds. –

(1) There shall be a fund to be known as the "Personal Data Protection Fund" solely managed by the Commission to bear its expenses and for running the functions of the Commission 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 under the instructions of the Finance division.

(3) The Personal Data Protection Fund shall be financed from the following sources, namely:

(a) An initial grant in the form of seed money from the Federal Government;

(b) Foreign aid, grants, and loans negotiated and raised, or otherwise obtained by the Commission without compromising its independence and 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.

46. Maintenance of accounts and audit. -

(1) The accounts of the Commission shall be maintained in such form and 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 furnish such explanations and information as the Auditor-General or any other officer authorised by him on this behalf may require for audit.

(4) Copies of the Auditor-General's report on the accounts shall be provided to the Commission, and the Federal Government shall make it available for public inspection on the website of the Commission.

(5) The Commission may, in addition to the audit under sub-section (1), require its accounts to be audited by any other external auditors.

47. Co-operation with international organisations. –The Commission may, subject to the prior approval of the Federal Government, shall cooperate with any foreign authority or international organisation in the field of data protection/data privacy/data theft/unlawful data transfer on the terms and conditions of any program or agreement for cooperation to which such authority or organisation is a party, or pursuant to any other international agreement made or after the commencement of this Act.

CHAPTER IX
COMPLAINT AND OFFENCES

48. Unlawful processing of personal data. –

(1) Whosoever processes or disseminates or discloses any personal data in violation of the provisions of this Act shall be punished with a fine up to 125,000 USD or an equivalent amount in Pakistani Rupees and in case of subsequent unlawful processing of personal data, the fine may be raised up to 250,000 USD or an equivalent amount in Pakistani Rupees.

(2) In case, where the offence is committed under sub-section (1) and relates to sensitive personal data the offender may be punished with a fine of up to 500,000 USD or an equivalent amount in Pakistani Rupees.

(3) In case, where the offence is committed under sub-section (1) and relates to critical personal data, the offender may be punished with a fine of up to 1,000,000 USD or an equivalent amount in Pakistani Rupees or as the Commission deems appropriate.

49. Failure to adopt data security measures. – Whosoever fails to adopt adequate security measures to ensure data security, as per the provisions laid down in this Act, Rules, and regulations, shall be punished with a fine of up to 50,000 USD or an equivalent amount in Pakistani Rupees.

50. Issue enforcement orders and impose penalties. –

(1) When an individual fails to comply with the orders of the Commission or the court when he is required to obey, shall be punished with a fine of up to 50,000 USD or an equivalent amount in Pakistani Rupees.

(2) Where a data controller and/or data processor contravenes with 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 a written notice within fifteen days require data controller and/or data Processor reasons for the non-issuance of the enforcement order.

(3) The notice referred to in sub-section (2) shall specify the nature of the contravention and adequate steps to be taken by the licensee for the redressal of the contravention.

(4) Where anyone fails to: -

(a) respond to the notice referred to in sub-section (2); or

(b) satisfy the Commission about the alleged contravention; or

(c) remedy the contravention within the time allowed by the Commission may by a written order and furnishing reasons for that shall: -

(i) levy fine which may extend to 2,000,000 USD or an equivalent amount in Pakistani Rupees; or

(ii) suspend or terminate the registration and impose additional conditions.

(5) Notwithstanding anything mentioned above, the legal person shall be punished with a fine not exceeding 1% of its annual gross revenue in Pakistan or 200,000 USD whichever is higher or an equivalent amount in Pakistani Rupees or as may be assessed by the Commission.

51. Complaint. –

(1) Any individual or relevant person may file a complaint before the Commission against any violation of personal data protection rights as granted under this Act, misconduct of any data controller, data processor, or their processes which involves: -

a) a breach of the data subject's consent to process data;

b) a breach of obligations of the data controller 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 subject; 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 simplified 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 and matters ancillary thereto 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 under intimation to 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 controller or data processor, after conducting an initial evaluation against whom the complaint has been made by providing him 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 controller 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 controller.

(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 controller or processor fails to respond to the Commission or execute its orders, the Commission may initiate enforcement proceedings as per Rules prescribed under this Act.

52. 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 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 X
MISCELLANEOUS

53. Temporary provisions. – (1) All data controllers and data processors shall adopt necessary security measures within six months from the day on which this Act comes into force.

54. Power to make Rules. –

(1) The Federal Government may, 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 provisions, these Rules may empower the Federal Government to: -

a) prepare and encourage data processors and data controllers to devise suitable codes of conduct and ethics;

b) verify the compliance of suitable codes with applicable laws;

c) seek views of the data controller and data processors in any manner related to the personal data;

d) contribute to the publicity and enforcement of suitable 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 controllers and data processors;

g) Matters connected or ancillary thereto.

(3) All public and regulatory authorities including but not limited to 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.

55. Power to make regulations. –The Commission shall issue regulations for exercising its powers to carry out the functions of the Commission, for internal working, appointment, promotion, termination, terms and conditions of its employees, which shall not contravene with any provision of this Act or the Rules made thereunder.

56. Relationship of the Act with other laws. –The provisions of this Act shall not contravene any other law on the subject for the time being in force. The sections of this Act will serve as bare minimum provisions and wherever there is any other applicable law on the subject, the provisions that have greater effect will prevail.

57. Indemnity. - No suit, prosecution, or other legal proceedings shall lie against the Commission or any member or employee, or consultant of the Commission in respect of anything done or intended to be done by the Commission in good faith under this Act.

58. Removal of difficulties. – (1) 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, shall make such provisions not inconsistent with the provisions of this Act as necessary for removing the difficulty.

59. Dissolution. – (1) No provision of law relating to the winding up of the bodies corporate shall apply to the Commission, and the Commission shall not be wound up except by order of the Federal Government, and in such manner, as the Federal Government may direct.