PERSONAL DATA PROTECTION BILL 2018

I N D E X

Chapter 1
Preliminary

1. **Short title and commencement**
2. **Definitions**
3. **Scope and applicability**

Chapter II
Processing of Personal Data and Obligations of Data Controller

4. **Protection of personal data**
5. **General requirements for personal data processing**
6. **Notice to the data subject**
7. **Non-disclosure of personal data**
8. **Security requirements**
9. **Data retention requirements**
10. **Data integrity and access to data**
11. **Record to be kept by data controller**

Chapter III
Rights of Data Subject

12. **Right of access to personal data**
13. **Compliance with data access request**
14. **Circumstances where data controller may refuse to comply with data access request**
15. **Right to correction of personal data**
16. **Compliance with data correction request**
17. **Circumstances where data controller may refuse to comply with data correction request**
18. **Notification of refusal to comply with data correction request**
19. **Right to withdraw consent to process personal data**
20. **Extent of disclosure of personal data**
21. **Right to prevent processing likely to cause damage or distress**
22. **Rights of foreign data subjects**

Chapter IV
Processing of Sensitive Personal Data

23. **Processing of sensitive personal data**

Chapter V
Exemptions

24. Repeated collection of personal data in same circumstances
25. Exemption
26. Power to make further exemption

Chapter VI
The Commission

27. National Commission for Personal Data Protection (NCPDP)
28. Functions of the Commission
29. Powers of the Commission
30. Meetings of the Commission
31. Funds

Chapter VII
Complaint and Offences

32. Unlawful Processing of personal data
33. Failure to adopt appropriate data security measures
34. Failure to comply with orders
35. Corporate liability
36. Complaint
37. Prosecution
38. Appeal
39. Offences to be bailable and compoundable

Chapter VIII
Miscellaneous

40. Temporary provisions
41. Power to make rules
42. Relationship of the Act with other laws
43. Removal of difficulties

PERSONAL DATA PROTECTION BILL 2018

A Bill

to protect people against the violation of their privacy by processing of personal data.

Whereas it is expedient to provide for the processing, obtaining, holding, usage and disclosure of data relating to Pakistani citizens while respecting the rights, freedoms and dignity of natural persons with special regard to their right to privacy, secrecy and personal identity and for matters connected therewith and ancillary thereto;

Now therefore it is enacted as follows:

CHAPTER I
PRELIMINARY

1. **Short title, extent and commencemen**t.—(1) This Act may be called the Personal Data Protection Act, 2017.

(2) It extends to the whole of Pakistan.

(3) It shall come into force after one year from the date of its promulgation or such other date not falling beyond two years from the date of its promulgation as the Federal Government may determine through a notification in the Official Gazette providing at least three months advance notice of the effective date.

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

(a) "Commission" means the National Commission for Personal Data Protection (NCPDP) established under section [] of the Act;

(b) "commercial transaction" means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance;

(c) "data" means information which is intentionally processed by means of equipment operating automatically or otherwise in response to instructions as part of a relevant data filing system and includes any representation of data that can be processed electronically;

(d) "data controller" means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor;

(e) "data processor", in relation to personal data, means any person, other than an employee of the data controller, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes";

(f) "data subject" means an individual who is the subject of the personal data;

(g) "personal data" means any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any sensitive personal data and expression of opinion about the data subject which—

(i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

(ii) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

(iiii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

;

Provided that anonymised, encrypted or pseudonymized data which is incapable of identifying an individual is not personal data.

(h) "processing", in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including—

(i) the organization, adaptation or alteration of personal data;

(ii) the retrieval, consultation or use of personal data; and

(iii) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or

(iv) the alignment, combination, correction, erasure or destruction of personal data;

(j) "third party", in relation to personal data, means any person other than—

(i) a data subject;

(ii) a relevant person in relation to a data subject;

(iii) a data controller;

(iv) a data processor; or

(v) a person authorized in writing by the data controller to process the personal data under the direct control of the data controller;

(k) "data filing system" means any set of data structured according to specific criteria suitable to ease processing of data;

(l) "relevant filing system" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set of information is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;

(m) "relevant person" in relation to a data subject means (a) in the case of a data subject who is below the age of 18 years, the parent or a guardian appointed by a court of competent jurisdiction; (b) in case of a data subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs; or (c) a person authorized by the data subject to make a data access or data correction request or both such requests.

(n) "rules" means rules made under this Act; and

(n) "sensitive personal data" means personal data consisting of information revealing racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership in political parties, trade unions, organizations and associations with a religious, philosophical, political or trade-union, biometric or genetic data, or provide information as to the health or sexual life of an individual, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings and financial,

or any other personal data as the Commission may determine by order published in the official Gazette;

(o) "vital interests" means matters relating to life, death or security of a data subject;

3. Scope and applicability.— (1) This Act applies to—
(a) any person who processes; and
(b) any person who has control over or authorizes the processing of,
any personal data relating to Pakistani citizens .

(2) Subject to subsection (1), this Act applies to a person in respect of personal data if—

(a) the person is established in Pakistan and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; and

(b) the person is not established in Pakistan, but uses equipment in Pakistan for processing the personal data otherwise than for the purposes of transit through Pakistan.

(3) A person falling within clause (b) of subsection (2) shall nominate for the purposes of this Act a representative established in Pakistan.

(4) For the purposes of subsections (2) and (3), each of the following is to be treated as established in Pakistan:
(a) an individual whose physical presence in Pakistan shall not be less than one hundred and eighty days in one calendar year;
(b) a body incorporated under the Companies Act 2017 (Act XIX of 2017);
(c) a partnership or other unincorporated association formed under any written laws in Pakistan; and
(d) any person who does not fall within paragraph (a), (b) or (c) but maintains in Pakistan—
(i) an office, branch or agency through which he carries on any activity; or
(ii) a regular practice.

(5) It shall not apply to:

(a) processing of personal data by a natural person in the course of a purely personal or household activity or family purposes;

(b) processing of personal data exclusively for journalistic, artistic or literary purposes subject to the conditions that:
(i) the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material;
(ii) the data controller reasonably believes 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 data controller reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes; and

(c) processing of personal data by a government entity solely for the purposes and to the extent provided under the relevant Act of the Parliament subject to the condition of ensuring security and secrecy for the protection and confidentiality of personal data;

Provided that the provisions of this Act shall apply to processing of personal data for commercial purposes by a government entity.

CHAPTER II
PROCESSING OF PERSONAL DATA AND OBLIGATIOINS OF THE DATA CONTROLLER AND DATA PROCESSORS

4. **Protection of personal data**.— The processing of personal data shall only be done in compliance with the provisions of this Act.

5. General requirements for personal data processing.- (1) A data controller shall not process personal data including sensitive personal dataof a data subject unless the data subject has given his consent to the processing of the personal data.

(2) Notwithstanding sub-section (1) , a data controller may process personal data about a data subject if the processing is necessary—
(a) for the performance of a contract to which the data subject is a party;
(b) for the taking of steps at the request of the data subject with a view to entering 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) in order to protect the vital interests of the data subject;
(e) for the administration of justice pursuant to an order of the court of competent jurisdiction;

(f) for legitimate interests pursued by the data controller; or
(g) for the exercise of any functions conferred on any person by or under any law.

(3) Personal data shall not be processed unless—
(a) the personal data is processed for a lawful purpose directly related to an activity of the data controller;
(b) the processing of the personal data is necessary for or directly related to that purpose; and
(c) the personal data is adequate but not excessive in relation to that purpose.

6. Notice to the data subject.- (1) A data controller shall by written notice inform a data subject—
(a) that personal data of the data subject is being processed by or on behalf of the data controller, and shall provide a description of the personal data to that data subject;
(b) the legal basis for the processing of personal data and time duration for which data is likely to be processed and retained thereafter;
the purposes for which the personal data is being or is to be collected and further processed;

(c) of any information available to the data controller as to the source of that personal data;
(d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data controller with any inquiries or complaints in respect of the personal data;
(e) of the class of third parties to whom the data controller discloses or may disclose the personal data;
(f) of the choices and means the data controller offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;
(g) whether it is obligatory or voluntary for the data subject to supply the personal data; and
(h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data.

(2) The notice under sub-section (1) shall be given as soon as reasonably possible by the data controller—
(a) when the data subject is first asked by the data controller 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 the personal data to a third party.

(3) A notice under sub-section (1) shall be in the national and English languages, and the individual shall be provided with a clear and readily accessible means to exercise his choice, where necessary, in the national and English languages.

7. Non-disclosure of personal data.- Subject to section 20, no personal data shall, without the consent of the data subject, be disclosed—
(a) for any purpose other than—
(i) the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or
(ii) a purpose directly related to the purpose referred to in subparagraph (i); or
(b) to any party other than a third party of the class of third parties as specified in clause (e) of sub-section (1) of section 6.

8. Security requirement.- (1) The Commission shall prescribe standards to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

(2) A data controller shall, when processing personal data, take practical steps to protect the personal data in the terms mentioned under sub-section (1) by having regard—
(a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;
(b) to the place or location where the personal data is stored;
(c) to any security measures incorporated into any equipment in which the personal data is stored;

(d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
(e) to the measures taken for ensuring the secure transfer of the personal data.

(2) Where processing of personal data is carried out by a data processor on behalf of the data controller, the data controller shall, for the purpose of protecting the personal data in the terms mentioned at sub-section (1) ensure that the data processorundertakes to adopt applicable technical and organizational security standards governing processing of personal data, as prescribed by the Commission

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

9. Data Retention requirements.- (1) The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.

(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.

10. Data integrity and access to data.- (1) A data controller shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.

(2) A data subject shall be given access to his personal data held by a data controller and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this Act.

11. Record to be kept by data controller (1) A data controller shall keep and maintain a record of any application, notice, request or any other information relating to personal data that has been or is being processed by him.
(2) The Commission may determine the manner and form in which the record is to be maintained.

12. **Prohibition on transfer of personal data**.- (1) Personal data shall not be transferred to any unauthorized person or system:

Provided that if personal data is required to be transferred to any system located beyond territories of Pakistan or system that is not under the direct control of any of the governments in Pakistan, it shall be ensured that the country where the data is being transferred offers personal data protection equivalent to the protection provided under this Act and the data so transferred shall be processed in accordance with this Act and, where applicable, the consent given by the data subject.

13. **Personal data breach notification**._(1) In the event of a personal data breach, data controller shall without undue delay and where reasonably possible, not beyond 72 hours of

becoming aware of the personal data breach, notify the Commission in respect of the personal data breach except where the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
(2) In the event of delay in notifying personal data breach beyond 72 hours, the personal data breach notification to the Commission shall be accompanied by reasons for the delay.
(3) The personal data breach notification shall at least provide 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 personal data records concerned;
b. name and contact details of the data protection officer or other contact point where more 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 may provide the above above listed information as per sub-section (3) in phases without undue delay, where it is not possible to provide the information at the same time.
(5) The data controller shall maintain record of any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.
(6) The data processor shall also follow the personal data breach notification requirements under this section in event of becoming aware of a personal data breach.

CHAPTER III
RIGHTS OF DATA SUBJECTS

14. Right of access to personal data.- (1) An individual is entitled to be informed by a data controller whether personal data of which that individual is the data subject is being processed by or on behalf of the data controller.

(2) A requestor may, upon payment of a prescribed fee, make a data access request in writing to the data controller—
(a) for information of the data subject's personal data that is being processed by or on behalf of the data controller; and
(b) to have communicated to him a copy of the personal data in an intelligible form.

(3) A data access request for any information under sub-section (2) shall be treated as a single request, and a data access request for information under clause (a))of sub-section (2) shall, in the absence of any indication to the contrary, be treated as extending also to such request under clause (b) of subsection (2).

(4) Where a data controller does not hold the personal data, but controls the processing of the personal data in such a way as to prohibit the data controller who holds the personal data from complying, whether in whole or part, with the data access request under subsection (2) which relates to the personal data, the first mentioned data controller shall be deemed to hold the personal data and the provisions of this Act shall be construed accordingly.

15. Compliance with data access request.- (1) Subject to sub-section (2) and section 14, a data controller shall comply with a data access request under section 12 not later than [thirt] 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 specified in subsection (1) shall before the expiration of that period—
(a) by notice in writing inform the requestor that the data controller is unable to comply with the data access request within such period and the reasons why the data controller is unable to do so; and
(b) comply with the data access request to the extent that the data controller is able to do so.

(3) Notwithstanding subsection (2), the data controller shall comply in whole with the data access request not later than fourteen days after the expiration of the period stipulated in subsection (1).

16. Circumstances where data controller may refuse to comply with data access request.- (1) A data controller may refuse to comply with a data access request under section 12 if—
(a) the data controller is not supplied with such information as the data controller may reasonably require—
(i) in order to satisfy itself as to the identity of the requestor; or
(ii) where the requestor claims to be a relevant person, in order to satisfy itself—
(A) as to the identity of the data subject in relation to 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) that other 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 the consent of the other individual;
(c) subject to subsection (3), any other data controller controls the processing of the personal data to which the data access 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 access request;
(d) providing access may constitute a violation of an order of a court;
(e) providing access may disclose confidential information relating to business of the data controller; or
(f) such access to personal data is regulated by another law.

(2) In determining for the purposes of clause (ii) of clause (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 with a view to seeking 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 so as to excuse the data controller from complying with the data access request under subsection (2) of section 15 to any extent that the data controller can comply with the data access request without contravening the prohibition concerned.

17. Right to correct personal data.- (1) Where—
(a) a copy of the personal data has been supplied by the data controller in compliance with the data access request under section 12 and 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 being held by the data controller is inaccurate, incomplete, misleading or not up-to-date,
the requestor or data subject, as the case may be, may make a data correction request in writing to the data controller that the data controller makes the necessary correction to the personal data.

(2) Where a data controller does not hold the personal data, but controls the processing of the personal data in such a way as to prohibit the data controller who holds the personal data from complying, whether in whole or in part, with the data correction request under subsection (1) which relates to the personal data, the first-mentioned data controller shall be deemed to be the data controller to whom such a request may be made and the provisions of this Act shall be construed accordingly.

18. Compliance with data correction request.- (1) Subject to subsections (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 personal data as corrected; and
(c) subject to subsection (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 using the personal data for the purpose, including any directly related purpose, for which the personal data was disclosed to the third party,
take all practicable steps to supply the third party with a copy of the personal data so corrected accompanied by a notice in writing 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 subsection (1) shall before the expiration of that period—
(a) by notice in writing inform the requestor that he is unable to comply with the data correction request within such period and the reasons why he is unable to do so; and
(b) comply with the data correction request to the extent that he is able to do so.

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

(4) A data controller is not required to comply with paragraph (1)(c) in any case where the disclosure of the personal data to a third party consists of the third party's own inspection of a register—
(a) in which the personal data is entered or otherwise recorded; and
(b) which is available for inspection by the public.

(5) Where a data controller is requested to correct personal data under subsection (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.

19. Circumstances where data controller may refuse to comply with data correction request.- (1) A data controller may refuse to comply with a data correction request under section 17 if—
(a) the data controller is not supplied with such information as it may reasonably require—
(i) in order to satisfy itself as to the identity of the requestor; or
(ii) where the requestor claims to be a relevant person, in order to satisfy itself—
(A) as to the identity of the data subject in relation to whom the requestor claims to be the relevant person; and
(B) that the requestor is the relevant person in relation to the data subject;
(b) the data controller is not supplied with such information as it may reasonably require to ascertain 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 subsection (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 so as to excuse the data controller from complying with subsection (1) of section 17 in relation to the data correction request to any extent that the data controller can comply with that subsection without contravening the prohibition concerned.

20. Notification of refusal to comply with data correction request.- (1) Where a data controller who pursuant to section 19 refuses to comply with a data correction request under section 17, it shall, not later than thirty days from the date of receipt of the data correction request, by notice in writing, inform the requestor—
(a) of the refusal and the reasons for the refusal; and
(b) where clause (e) of sub-section (1) of section 18 is applicable, of the name and address of the other data controller concerned.

(2) Without prejudice to the generality of subsection (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) of the matters in respect of which the expression of opinion is considered by the requestor to be inaccurate, incomplete, misleading or not up-to-date; and

(ii) in such a way that the personal data cannot be used by any person without the note being drawn to the attention of and being available for inspection by that person; and

(b) attach a copy of the note to the notice referred to in subsection (1) which relates to the data correction request.

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

21. Withdrawal of consent to process personal data.- (1) A data subject may by notice in writing withdraw his consent to the processing of personal data in respect of which he is the data subject.

(2) The data controller shall, upon receiving the notice under subsection (1), cease the processing of the personal data.

(3) The failure of the data subject to exercise the right conferred by subsection (1) does not affect any other rights conferred on him by this Part.

(4) A data controller who contravenes subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding one million rupees or to imprisonment for a term not exceeding one year or to both.

22. Extent of disclosure of personal data.- Notwithstanding section 7, 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 to be disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances:

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

(b) the disclosure —

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

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

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

(d) the data controller acted in the reasonable belief that he would have 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 as being in the public interest in circumstances as determined by the Commission in advance of the disclosure.

23. Right to prevent processing likely to cause damage or distress (1) Subject to subsection (2), a data subject may, at any time by notice in writing to a data controller, referred to as the "data subject notice", require the data controller at the end of such period as is reasonable in the circumstances, to—

(a) cease the processing of or processing for a specified purpose or in a specified 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 substantial distress to him or to another person; and

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

(2) Subsection (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 the taking of steps at the request of the data subject with a view to entering 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) in order 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 through publication in the Official Gazette.

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

(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 subsection (3) (b), the data subject may submit an application to the Commission to require the data controller to comply with the data subject notice.

(5) Where the Commission is satisfied that the application of the data subject under subsection (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.

24. Rights of foreign data subjects.— Foreign data subject shall have all his rights, if any provided under the laws of the country or territory where the foreign data has been collected or data subject resides in so far as consistent with this Act, only against the data controller.

25. Right to erasure.- (1) The data subject shall have the right to obtain from the data controller the erasure of personal data concerning him without undue delay and the data

controller 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 in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based in accordance with section 21 (1) and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to sub-section (1) of section 23and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to sub-section (2) of section 23;

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

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

(2) Where the data controller has made the personal data public and is obliged pursuant to subsection (1) to erase the personal data, the data controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform data processors which are processing the personal data that the data subject has requested the erasure by such data controllers of any links to, or copy or replication of, those personal data.

(3) 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 for 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 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.

CHAPTER IV
PROCESSING OF SENSITIVE PERSONAL DATA

26. Processing of sensitive personal data.- (1) Subject to subsection (2) of section 5, a data controller shall not process any sensitive personal data of a data subject except in accordance with the following conditions:
(a) the data subject has given his explicit consent to the processing of the personal data; and
(b) the processing is necessary—
(i) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment; or

(ii) in order 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) in order 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 and is undertaken by—

(A) a healthcare professional; or

(B) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;

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

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

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

(viii) for the administration of justice pursuant to 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; or

(c) the information contained in the personal data has been made public as a result of steps deliberately taken 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 subsection (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 in clauses (i), (viii) or (ix) of clause (b) of subsection (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

Explanation.- For the purposes of this section—

"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;

"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 the giving of medical, health, dental, pharmaceutical or any other healthcare services authorised to provide such services under the laws of Pakistan.

CHAPTER V
EXEMPTIONS

27. Repeated collection of personal data in same circumstances.- (1) Where a data controller—

(a) has complied with the requirements of this Act in respect of the collection of personal data from the data subject, referred to as the "first collection"; and

(b) on any subsequent occasion again collects personal data from that data subject, referred to as the "subsequent collection",

the data controller shall not be required to comply with the requirements of section 7 in respect of the subsequent collection if—

(A) 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

(B) not more than twelve months have elapsed between the first collection and the subsequent collection.

(2) For the avoidance of doubt, it is declared that subsection (1) shall not operate to prevent a subsequent collection from becoming a first collection if the data controller concerned has complied with the provisions of the notice and consent in respect of the subsequent collection.

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

(2) Subject to section [], personal data—

(a) processed for—

(i) the prevention or detection of crime or for the purpose of investigations;

(ii) the apprehension or prosecution of offenders; or

(iii) the assessment or collection of any tax or duty or any other imposition of a similar nature,

shall be exempted from sections 5, 6, 7 and subsection (2) of section 8 of this Act and such other related provisions of this Act as may be prescribed by the Commission for specific purposes;

(b) processed in relation to information of the physical or mental health of a data subject shall be exempted from subsection (2) of section 8 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 5, 6, 7 and subsection (2) of section 8 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) that is necessary for the purpose of or in connection with any order or judgment of a court shall be exempted from sections 5, 6, 7 and subsection (2) of section 8 of the Act and other related provisions of this Act;

(e) processed for the purpose of discharging regulatory functions shall be exempted from sections 5, 6, 7 and subsection (2) of section 8 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) processed only for journalistic, literary or artistic purposes shall be exempted from sections 5, 6, 7, 8, 9, 10, 11 and other related provisions of this Act, provided that—

(i) the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material;

(ii) the data controller reasonably believes 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 data controller reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.

29. Power to make further exemptions.- (1) The Federal Government may, upon the recommendation of the Commission, by order published in the official Gazette exempt the application of any provision of this Act to any data controller or class of data controller.

(2) The Federal Government may impose any terms or conditions as it thinks fit in respect of any exemption made under subsection (1).

(3) The Federal Government may at any time, on the recommendation of the Commission, by order published in the Gazette, revoke any order made under subsection (1).

(4) An appeal against an order passed by the Federal Government under subsection (1) shall lie to the High Court.

CHAPTER VI
THE COMMISSION

30. Commission for Personal Data Protection ._(1) Within six months of coming into force of this Act, the Federal Government shall establish the National Commission for Personal Data Protection (NCPDP).

(2) The Commission shall be a corporate body, having perpetual succession which can sue and be sued in its own name and shall enjoy operational and administrative autonomy, except as specifically provided for under this Act.

(3) The Commission shall comprise of three Commissioners, to be appointed by the Prime Minister as follows:

(a) One Commissioner shall be a person who has been or is qualified to be a judge of High Court;

(b) One Commissioner shall be a person having master degree in computer sciences or telecommunications and fifteen years of experience in the field of information technology, telecommunications or computer sciences; and

(c) One Commissioner shall be a person from civil society having a degree based on sixteen years of education from a recognized institution and fifteen years of experience in the field of mass communication, academics and civil rights.

(5) The Commission shall be headed by a Chairman, who shall be nominated by the Federal Government from amongst the three Commissioners.

(6) The Commissioners including the Commissioner nominated as Chairman shall hold office for a term of four years from the date on which they assume office and shall not be eligible for re-appointment.

(7) The Commissioner shall be entitled to such remuneration and other benefits during the term of his office as may be admissible to a judge of the Islamabad High Court including pension benefits:

Provided that the pension benefits shall not be available to any person who accepts any other office of profit in connection with the affairs of the government of Pakistan or any provincial government.

(8) A Commissioner shall not hold any other office of profit including any other public office or be connected with any political party during his appointment to the Commission and, once appointed, a Commissioner shall work on full time basis and may not run any business or pursue any other profession during his tenure as Commissioner.

(9) A person who has accepted and served as a Commissioner shall not accept any other office of profit in connection with the affairs of the government of Pakistan or any provincial government for a period of three years.

(10) A Commissioner may be removed from office by the Federal Government if it is found upon an inquiry conducted by the Federal Public Service Commission on directions of the Prime Minister that he is guilty of misconduct or suffers from mental or physical incapacity for performance of his duties as a Commissioner.

31. Functions of the Commission.- (1) The Commission shall be responsible to enforce protection of personal data and shall entertain complaints under this Act.

(2) Without prejudice to the generality of the foregoing function, the Commission shall particularly perform the following functions.-

(a) receive and decide complaints with regard to infringement of personal data protection including violation of any provision of this Act;

(b) examine various laws, rules, policies, bye-laws, regulations or instructions in relation to protection of personal data and may suggest amendments to bring the law in conformity with the provisions of the Act;

(c) take steps to create public awareness about personal data protection rights and filing of complaints against infringement of these rights under this Act;

(d) engage, support, guide, facilitate, train and persuade data controllers, data processors to ensure protection of personal data under this Act; and

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

32. Powers of the Commission: The Commission shall have all powers, direct or incidental, as are necessary to undertake its functions as provided for in this Act, and the power to acquire, hold and dispose of property including the powers to:-

(a) formulate, approve and implement policies, procedures and regulations for its internal administration, operations, human resource management, procurements financial management and partnerships;

(b) prescribe schedule of costs and the mode of payment for filing of complaint and its format;

(c) seek information from data controllers in respect of data processing under this Act and impose penalties for non-observance of data security practices and non-compliance of the provisions of this Act;

(d) order a data controller to take such reasonable measures as it may deem necessary to remedy an applicant for any failure to implement the provisions of this Act;

(e) summon and enforce the attendance of witnesses and compelling them to give oral and written evidence under oath

33. Meetings of the Commission.- (1) A meeting of the Commission shall be convened and chaired by the Chairman/Chief Data Protection Commissioner.

(2) In case the position of Chairman/Chief Data Commissioner is vacant or if he is not available due to any cause, the Federal Government may direct any other Commissioner to serve as acting Chief Data Protection Commissioner who may also convene and chair a meeting of the Commission.

(3) Two Commissioners shall constitute quorum for a meeting of the Commission.

34. Funds: The Federal Government shall make such a budgetary allocation to the Commission as may be required by the Commission for effective exercise of its powers and functions.

CHAPTER VII
COMPLAINT AND OFFENCES

35. Unlawful processing of personal data.— Anyone who processes or cause to be processed, disseminates or discloses personal data in violation of any of the provisions of this

Act shall be punished with fine upto three million rupees and in case of a subsequent unlawful processing of personal data, the fine may exceed to ……

(2) In case the offence committed under sub-section (1) relates to sensitive data the offender may be punished with fine upto five million rupees.

36. Failure to adopt appropriate data security measures.— Anyone who fails to adopt the security measures that are necessary to ensure data security, when he is required to do so, in violation of the provisions laid down in this Act and the rules made thereunder shall be punished with fine upto one million rupees.

37. Failure to comply with orders.— Anyone who fails to comply with the orders of the commission or the court when he is required to do so, shall be punished with fine upto five hundred thousand rupees.

38. **Corporate liability.—** A person shall be held liable for a non-compliance committed on his instructions or for his benefit or lack of required supervision by any individual, acting either individually or as part of a group of persons, who has a leading position within it, based on a power of representation of the person; an authority to take decisions on behalf of the person; or an authority to exercise control within it. The person shall be punished with fine not exceeding five million rupees.

Provided that such punishment shall not absolve the liability of the individual, who has committed the offence.

39. Complaint.— (1) Any aggrieved person may file a complaint before the Commission against any violation of personal data protection rights as granted under this Act, conduct of any data controller, data processor or their processes which a complainant regards as involving:-
(a) a breach of data subject's consent to process data;
(b) a breach of obligations of the data controller or the data processor in 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 protection of personal data.

(2) The complainant may file a complaint on a plain paper or on 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 reasonable fee for filing or processing of the complaint, as prescribed under this Act and shall also facilitate on-line receipt of complaints.

(4) The Commission shall acknowledge the receipt of 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 explanation from the data controller or data processor against whom the complaint has been made by affording him reasonable time and opportunity to be heard through an efficient mode of communication; and
(b) contact, if deemed necessary, the complainant 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 it may issue directions to stop breach of data protection rights of a data subject without first seeking comments from the concerned data processor and data controller, as the case may be. The Commission may employ electronic means of communication to dispose of complaints and shall maintain appropriate record of such communications. The Commission shall, as soon as possible establish an online facility to receive, process, manage and dispose of complaints in an efficient and cost effective manner.

(7) In case of failure of the data collector or data processor, as the case may be, to respond to the Commission or to execute its orders, the Commission may initiate enforcement proceedings as per rules prescribed under this Act.

40. Judicial Recourse.— (1) Any person dissatisfied with the processing of his compliant at the Commission, may seek directions from the High Court in whose territorial jurisdiction the aggrieved person is permanently or temporarily residing.

(2) On receipt of a complaint under sub-section (1), the High Court may seek report from the Commission and may also restrain the data controller, data processor or any other person involved in data processing to refrain from processing, dissemination or disclosure of such personal data:

Provided that no restraining order under this section shall be issued by the court unless it is satisfied that:

a. sufficient grounds exist to believe that data processing is being carried out in violation of the law;

b. the complaint is accompanied with an affidavit of the complainant verifying the contents of the complaint; and

c. the complainant is likely to suffer irreparable loss.

CHAPTER VIII
MISCELLANEOUS

40. Temporary provisions.— All data controllers and data processors shall adopt necessary security measures within [six months] from the day on which this Act comes into force.

41. 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 controllers;
(b) verify the compliance of such codes with applicable laws;
(c) seek views of data controller 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 controllers and data processors.

(3) All public and regulatory authorities especially in the banking, insurance, telecommunication, legal and health sector shall assist the Commission in exercise and performance of its powers and functions under this Act.

42. 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.

43. 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 non inconsistent with the provisions of the Act as may appear to be necessary for removing the difficulty.

Statement of Objects

The Constitution of the Islamic Republic of Pakistan guarantees privacy of home alongside dignity of every man and woman as their fundamental right under its Article 14. Digitization of businesses and various public services employing modern computing technologies involves processing of personal data. The growth of technological advancements have not only made it easier to collect personal data but also enabled processing of personal data in so many ways that were not possible in the past. In today's digital age, personal data has become an extremely valuable commodity and for many businesses the sole source of their income is the personal data of users they generate. The personal data is often being collected, processed and even sold without knowledge a person. In some cases, such personal information is used for relatively less troublesome commercial purposes e.g. targeted advertising etc. However, the data so captured or generated can be misused in many ways e.g. blackmail, behavior modification, phishing scams etc.

In order to realize the goal of full scale adoption of e-government and delivery of services to the people on their doorsteps, and increase users' confidence in the confidentiality and integrity of government databases, it is essential that the users' data is fully protected from any unauthorized access or usage and remedies are provided to them against any misuse of their personal data. Additionally, accelerated increase in the use of broadband with the advent of 3G/4G in Pakistan led to an increasingly enhanced reliance on technology calling for protection of people's data against any misuse, thus maintaining their confidence in the use of new technologies without any fear.

Whereas sectoral arrangements/frameworks exist in Pakistan that provide for data protection and Prevention of Electronic Crimes Act 2016 (Act No.XL of 2016) deals with the crimes relating to unauthorized access to data, there is a need for putting in place a comprehensive legal framework in line with our Constitution and international best practices for personal data protection. Protecting personal data is also necessary to provide legal certainty to the businesses and public functionaries with regard to processing of personal data in their activities. The desired legal framework would clearly spell out the responsibilities of the data collectors and processors as well as rights and privileges of the data subjects along with institutional provisions for regulation of activities relating to the collections, storing, processing and usage of personal data.