MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION

PERSONAL DATA PROTECTION BILL 2021

CONSULTATION DRAFT: V.25.08.2021

TABLE OF CONTENTS

STATEMENT OF OBJECTS

The Constitution of the Islamic Republic of Pakistan guarantees the privacy of the home alongside the dignity of every man and woman as their fundamental right under Article 14. Digitization of businesses and various public services employing modern computing technologies involves the processing of personal data. The growth of technological advancements has not only made it easier to collect personal data but also enabled the 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. Personal data is often being collected, processed, and even sold without the knowledge of 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.

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 data. Additionally, the accelerated increase in the use of broadband with the advent of Next Generation Mobile Service and Networks in Pakistan led to an increasingly enhanced reliance on technology calling for the 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 provides 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 concerning the processing of personal data in their activities. The desired legal framework would spell out the responsibilities of the data controllers 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.

PERSONAL DATA PROTECTION BILL 2021

A Bill to govern the collection, processing, use, and disclosure of personal data and to establish and making provisions about offenses relating to violation of the right to data privacy of individuals by collecting, obtaining, or processing of personal data by any means.

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

Now therefore it is enacted as follows:

CHAPTER I

PRELIMINARY

1 SHORT TITLE, EXTENT AND COMMENCEMENT

1.1 This Act may be called the Personal Data Protection Act, 2021.

1.2 It extends to the whole of Pakistan.

1.3 It shall come into force 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) **"anonymized data"** means information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable;

b) **"Commission"** means the National Commission for Personal Data Protection (NCPDP) established under section 32 of the Act;

c) **"consent"** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the collecting, obtaining and processing of personal data relating to him or her;

d) **"critical personal data"** means and includes data relating to public service providers, unregulated e-commerce transactions and any data related to international obligations;

e) **"data controller"** means a natural or legal person or the government, who either alone or jointly has the authority to make a decision on the collection, obtaining, usage or disclosure of personal data;

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

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

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

i) **"Government"** means Government means federal government, provincial government and local governments;

j) **"legitimate interest"** means anything permitted under the law or permitted legislation;

k) **"personal data"** means any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller and/or data processor, including any sensitive personal data.

Provided that anonymized, or pseudonymized data which is incapable of identifying an individual is not personal data;

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

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

n) **"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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

o) **"public interest"** means any matter pertaining to 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 inconformity with laws of the land;

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

q) **"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 and/or data correction request;

r) **"requestor"** means anybody who makes request under this Act for any matter related or ancillary to this Act;

s) **"rules"** means rules made under this Act;

t) **"sensitive personal data"** means and includes data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, computerized national identity card, passports, biometric data, and physical, behavioral, psychological, and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, political affiliation, physical identifiable location, travelling details, pictorial or graphical still and motion forms, IP address and online identifier;

u) **"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;

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

3 SCOPE AND APPLICABILITY

3.1 This Act applies to

a) any person/government who processes or has control over or authorizes the processing of any personal data, provided the data controller or processor is established/present in Pakistan.
b) controller or processor digitally or non-digitally operational in Pakistan, but incorporated in any other jurisdiction and involved in commercial or non-commercial activity in Pakistan.
c) the processing of personal data by a controller and processor not established in Pakistan, but in a place where Pakistani law applies by virtue of private and public international law.
d) any data subject present in Pakistan.

CHAPTER II

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

4 PROTECTION OF PERSONAL DATA

4.1 The collection, processing and disclosure of personal data shall only be done as necessary in compliance with the provisions of this Act.

4.2 The data be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed.

5 GENERAL REQUIREMENTS FOR PERSONAL DATA COLLECTION AND PROCESSING

5.1 A data controller shall not process personal data including sensitive personal data of a data subject unless the data subject has given his consent to the processing of the personal data. A separate consent shall be obtained from the data subject for each purpose.

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

a) for the performance of a contract to which the data subject is a party;
b) for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;
c) in order to protect the vital interests of the data subject;
d) for the administration of justice pursuant to an order of the court of competent jurisdiction;
e) for legitimate interests pursued by the data controller; or
f) for the exercise of any functions conferred on any person by or under any law.

5.3 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

6.1 A data controller shall by written notice inform a data subject or where this is not practical, via a written notice provided by another data controller that exercises control over the same personal data—

a) that personal data of the data subject is being collected by or on behalf of a 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 restricting 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.

6.2 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.

6.3 A notice under sub-section (1) shall be in the national and/or 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

7.1 Subject to section 24, 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 REQUIREMENTS

8.1 The Commission, keeping in mind national interest, shall prescribe best international standards to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

8.2 A data controller or processor shall, when collecting or processing personal data take practical measures to protect the personal data in the terms mentioned under sub-section (1) by having regard 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;

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 the personal data.

8.3 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 processor undertakes to adopt applicable technical and organizational security international standards governing processing of personal data, as prescribed by the Commission.

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

8.5 Save as other related laws will also remain in the field in their respective domains.

9 DATA RETENTION REQUIREMENTS

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

9.2 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).

10 DATA INTEGRITY AND ACCESS TO DATA

10.1 A data controller shall take adequate steps to ensure that the required 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.

10.2 A data subject shall be given access to his personal data held by a data controller and data controller be liable 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

11.1 A data controller shall keep and maintain a record of each application, notice, request or any other information relating to personal data that has been or is being processed by him.

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

11.3 The data controller shall intimate to the Commission on regular basis the type of data they are collecting and the processing undertaken on the collective data. This is not applicable on situations where data collection is occasional unless the processing is likely to result in a risk to the rights and freedoms of data subject.

12 TRANSFER OF PERSONAL DATA

12.1 Personal data shall not be transferred to any unauthorized person or system and contrary to the provisions of the Act.

13 PERSONAL DATA BREACH NOTIFICATION

13.1 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 and the data subject 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 data subject.

13.2 In the event of delay in notifying personal data breach beyond 72 hours, the personal data breach notification to the Commission and the data subject shall be accompanied by valid reasons for the delay.

13.3 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.

13.4 The data controller shall maintain record of all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

13.5 The data processor shall also follow the personal data breach notification requirements provided under this section in event of becoming aware of a personal data breach.

14 CROSS BORDER TRANSFER OF PERSONAL DATA

14.1 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 government of Pakistan or entity/entities of Pakistan, it shall be ensured that the country where the data is being transferred offers personal data protection legal regime at least 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.

14.2 Critical Personal Data shall only be processed in a server or data centre located in Pakistan.

15 FRAMEWORK ON CONDITIONS FOR CROSS-BORDER TRANSFER OF PERSONAL DATA

15.1 Personal data other than those categorize as critical personal data may be transferred outside the territory of Pakistan under a framework (on conditions) to be devised by the Commission.

15.2 The Commission shall also devise a mechanism for keeping some components of the of sensitive personal data in Pakistan to which this act applies, provided that related to public order or national security.

CHAPTER III

RIGHTS OF DATA SUBJECTS

16 RIGHT OF ACCESS TO PERSONAL DATA

16.1 A data subject or relevant person 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.

16.2 A requestor may upon payment of a prescribed reasonable fee based on administrative cost 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.

16.3 Where a data controller has shared the data to another data processor/controller, the data controller possessed any consent of the data subject would be liable as provided under Section 16.2.

17 COMPLIANCE WITH DATA ACCESS REQUEST

17.1 Subject to sub-section (2) and section 14 a data controller shall comply with a data access request under section 10 not later than [thirty] days from the date of receipt of the data access request.

17.2 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.

17.3 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).

18 CIRCUMSTANCES WHERE DATA CONTROLLER MAY REFUSE TO COMPLY WITH DATA ACCESS REQUEST

18.1 A data controller may refuse to comply with a data access request under section 10 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) providing access may constitute a violation of an order of a court;
d) providing access may disclose confidential information relating to business of the data controller; or
e) such access to personal data is regulated by another law.

18.2 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.

18.3 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 10 to any extent that the data controller can comply with the data access request without contravening the prohibition concerned.

19 RIGHT TO CORRECT PERSONAL DATA

19.1 Where—

a) a copy of the personal data has been supplied by the data controller in compliance with the data access request under section 10 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.

19.2 Where a data controller has shared the data to another data processor/controller, the data controller possessed any consent of the data subject would be liable act upon under Section 19.1.

20 COMPLIANCE WITH DATA CORRECTION REQUEST

20.1 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.

20.2 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
f) comply with the data correction request to the extent that he is able to do so.

20.3 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).

20.4 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.

20.5 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.

21 CIRCUMSTANCES WHERE DATA CONTROLLER MAY REFUSE TO COMPLY WITH DATA CORRECTION REQUEST

21.1 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. 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.

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

22 NOTIFICATION OF REFUSAL TO COMPLY WITH DATA CORRECTION REQUEST

22.1 Where a data controller who pursuant to 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 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 21 is applicable, of the name and address of the other data controller concerned.

22.2 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.

22.3 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.

23 WITHDRAWAL OF CONSENT TO PROCESS PERSONAL DATA

23.1 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 at any point in time.

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

23.3 The withdrawal of the consent shall not affect the lawfulness of the processing based on consent before its withdrawal.

23.4 A data controller who contravenes subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding five million rupees.

24 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.

25 RIGHT TO PREVENT PROCESSING LIKELY TO CAUSE DAMAGE OR DISTRESS

25.1 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 a relevant person; and

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

25.2 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 ~~Authority~~ through publication in the Official Gazette.

25.3 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.

25.4 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 a complaint to the Commission to require the data controller to comply with the data subject notice.

25.5 Where the Commission is satisfied that the complaint 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.

26 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 personal data has been collected or data subject resides in so far as consistent with this Act.

27 RIGHT TO ERASURE

27.1 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 23 (1) and where there is no other legal ground for the processing; or
c) 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.

27.2 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 adequate steps, including technical measures, to inform data processors who are processing the personal data to get it erased, along with any links to, or copy or replication of, those personal data.

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

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation or 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.

28 GENERAL PROTECTED RIGHTS

Not contrary to any other law, the following rights of the data subject are protected under the Act.

a. Right to Data Portability

b. Right not to be subject to a decision based solely on automated processing, including profiling

CHAPTER IV

PROCESSING OF SENSITIVE PERSONAL DATA

29 PROCESSING OF SENSITIVE PERSONAL DATA

29.1 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 provided that this consent is not restricted by any other applicable law; and/or

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;

c) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

29.2 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 authorized to provide such services under the laws of Pakistan.

CHAPTER V
EXEMPTIONS

30 REPEATED COLLECTION OF PERSONAL DATA IN SAME CIRCUMSTANCES

30.1 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 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—

i. to comply with those provisions in respect of that subsequent collection would be to repeat, in the same circumstances, what was done to comply with that principle in respect of the first collection; and

ii. not more than twelve months have elapsed between the first collection and the subsequent collection.

30.2 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.

31 EXEMPTION

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

31.2 Subject to section [28] exemptions may be granted provided personal data is:-

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 by the relevant authority 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 under the Rules and Commission for specific purposes permitted under this Act;

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 subject to reasonable grounds, 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 processing of personal data in the interests of the security of the State provided that the processing of personal data shall not be permitted unless it is authorized pursuant to an express authorization by the Commission.

CHAPTER VI

THE COMMISSION

32 ESTABLISHMENT OF THE COMMISSION

32.1 Within six months of passage into force of this Act, the Federal Government shall, by notification in the official Gazette, establish a Commission to be known as the National Commission for Personal Data Protection (NCPDP) of Pakistan, to carry out the purposes of this Act.

32.2 The Commission shall be a statutory corporate body having perpetual succession and a common seal, and may sue and be sued in its own name and, subject to and for the purposes of this Act, may enter into contracts and may acquire, purchase, take and hold moveable and immovable property of every description and 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 and, shall enjoy operational and administrative autonomy, except as specifically provided for under this Act. The Commission shall be an autonomous body under the administrative control of the Federal government with its headquarters at Islamabad.

32.3 The Commission may setup its establishments including sub-offices at Provincial capitals and such other places, as it may deem necessary from time to time.

32.4 The Commission shall consist of five members, one of whom shall be an ICT expert of Data Protection field, a legal expert, strategic interest expert, a representative of civil society and a financial/accounting expert, respectively, to be appointed by the Federal Government for a term of four years and shall be eligible for reappointment for a similar term.

32.5 Provided that the Federal Government may increase the number of members of the Commission and prescribe their qualifications and mode of appointment.

32.6 The Federal Government shall, from amongst the members appointed under sub-section (4), appoint a member to be the Chairman of the Commission.

32.7 The Members of the Commission shall be paid salary and shall be entitled to the privileges of an officer in PM-I scale. The Member of the Commission shall not hold any other office of profit including any other public office or be connected with any political party or have any conflict of interest with regards to this Act during discharging his duties in the Commission as envisaged under the Act.

32.8 A Member of the Commission may resign from his office in writing addressed to the Federal Government, or may be removed from his office by the Federal Government, if on an inquiry conducted by the Federal Public Service Commission or is found unable to perform the functions of his office because of mental or physical disability or misconduct including corruption and dishonesty.

32.9 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 at sub-section (4).

32.10 The power of the Commission in the matters relating to its administration and the staff of the Commission shall be exercised by the Chairman including appointments of its employees, in accordance with regulations made by the Commission pursuant to section 37 and other relevant regulations made by the Commission from time to time.

32.11 The decision of the Commission shall, subject to sub-section (10), be taken with the concurrence of the majority of its members.

Notwithstanding anything contained in sub-section (10), no act or proceeding of the Commission shall be invalid by reason only of the existence of a vacancy in, or a defect in the constitution of the Commission.

33 FUNCTIONS OF THE COMMISSION

33.1 The Commission shall be responsible to protect the interest of the data subject and enforce protection of personal data, prevent any misuse of personal data, promote awareness of data protection and shall entertain complaints under this Act.

33.2 Without prejudice to the generality of the foregoing and other functions set out under this Act, the Commission shall particularly perform the following functions.-

a) Receiving and deciding complaints with regard to infringement of personal data protection including violation of any provision of this Act;
b) examining 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) taking steps to create public awareness about personal data protection rights and filing of complaints against infringement of these rights under this Act;
d) engaging, supporting, guiding, facilitating, training and persuading data controllers, data processors to ensure protection of personal data under this Act; and
e) ensuring that all of its decisions are based on established principles to structure or minimize discretion and ensure transparency and accountability.
f) monitoring and enforcing application of the provisions of this Act.
g) taking prompt and appropriate action in response to a data security breach in accordance with the provisions of this Act.
h) monitoring cross-border transfer of personal data under this Act.
i) monitoring technological developments and commercial practices that may affect protection of personal data and promoting measures and undertaking research for innovation in the field of protection of personal data.
j) advising to the Federal Government and any other statutory authority on measures that must be undertaken to promote protection of personal data and ensuring 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.

33.3 To make recommendations to the Federal Government on Policies with respect to Personal Data Protection in line with International best practices and National requirements.

33.4 To perform such other functions as the Federal Government may, from time to time, assign to it

34 POWERS OF THE COMMISSION

(1) The Commission shall have and exercise all powers as shall enable it to effectively perform its functions specified in section 32.

(2) In particular and without prejudice to the generality of the foregoing power, the Commission shall---

a) decide the complaint or pass any order and for this purpose, the Commission shall be deemed to be a Civil Court and shall have the same powers as are vested in 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 compliance framework for monitoring and enforcement in order to ensure transparency and accountability, subject to the measures including but not limited to the following:
    i. Privacy
    ii. Transparency
    iii. Security Safeguards
    iv. Personal Data Breach
    v. Data Protection Impact Assessment
    vi. Record Maintenance
    vii. Data Audits
    viii. Responsibilities of Data Protection Officer
    ix. Processing by entities other than Data Controller
    x. Classification of Data Controller
    xi. Grievance Redressal mechanism
    xii. Cross-border data sharing
    xiii. Cross Border Equivalence Mechanism and matters ancillary thereto
d) Identify big / large data controllers / processors, alongwith other categories, and define special measures for compliance in accordance with the provisions of the Act;
e) Formulate a Registration Framework for Data Controllers and Data Processors under the Act;
f) Take prompt and appropriate action in response to a data security breach in accordance with the provisions of the Act;
g) Powers of search and seizure while handling/ dealing with the compliant;
h) prescribe schedule of costs and the mode of payment for filing of complaint and its format;
i) 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;

j) 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; and

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

35 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 effective discharging of its functions under this Act.

(2) Whenever the Commission require any information from the data controller or data processor, the concern officer of the Commission it shall provide a written notice to the data controller or the data processor stating reason for such requisition in a specified manner and form in which such information may be provided.

36 MEETINGS OF THE COMMISSION

36.1 A meeting of the Commission shall be convened and chaired by the Chairman.

36.2 In case the position of Chairman is vacant or if he is not available due to any cause, the majority of the Members present can decide, who may convene and chair a meeting of the Commission.

36.3 Three Members shall constitute a quorum for a meeting of the Commission.

37 POWERS OF THE FEDERAL GOVERNMENT TO ISSUE POLICY DIRECTIVES.

37.1 The Federal Government may, as and when it considers necessary, issue policy directives to the Commission, not inconsistent with the provisions of the Act, on the matters relating to Personal Data Protection and all connected and ancillary matters therewith and the Commission shall comply with such directives.

38 APPOINTMENT OF EMPLOYEES.

38.1 For performance of its functions, the Commission may, from time to time, employee such persons and on such terms and conditions as deem necessary.

38.2 Without prejudice to the generality of the foregoing powers, the Commission may;

(a) appoint and remove its employees, officers and exercise discipline and control over them and any remuneration, salary or allowances and any such terms and conditions of service of such officers, employee, consultant and experts shall be such as may be prescribed.

(b) regulate and manage its internal organization, set up divisions within the Commission and make appropriate appointments to those divisions; and

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

39 MEMBERS AND EMPLOYEES.

The members and employees of the Commission shall be public servant within the meaning of section 21 of the Pakistan Penal Code (Act XLV of 1860).

40 SUBMISSION OF YEARLY REPORTS, RETURNS, ETC.

(1) As soon as possible after the end of every financial year but before the last date of September next following, the Commission shall submit a report to the Federal Government on the conduct of its affairs, including action taken for the 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 after the finalization of the audit report by the Auditor-General.

(3) For the purpose of carrying on its functions under this Act, the Federal Government may require the Commission to supply any return, statement, estimate, statistics or other information in respect of any matter under the control of the Commission or a copy of any document in the custody of the Commission.

41 FUNDS

41.1 There shall be a fund to be known as the "Personal Data Protection Fund" which shall vest in the Commission and shall be utilized by the Commission to meet all its expenses and charges in connection with its functions under this Act, including the payments of salaries and other remuneration to its employees.

41.2 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.

41.3 The Personal Data Protection Fund shall be financed from the following sources, namely:

(a) Loans and grants from the Federal Government and the Provincial Governments, including an initial grant of ……..million rupees by the Federal Government;

(b) Foreign aid, grants and loans negotiated and raised, or otherwise obtained by the Commission with the approval of the Federal Government.

(c) Fees / Registration Fee and other amounts received by the Commission from time to time.

(d) Income from the sale of moveable or immoveable property;

(e) Income from investments; and

(f) All other sums received or earned by the Commission.

42 MAINTENANCE OF ACCOUNTS AND AUDIT

(1) The accounts of the Commission shall be maintained in such form and in such manner as the Federal Government may determine in such manner as the Federal Government may determine in consultation with the Auditor –General of Pakistan.

(2) The accounts of the Commission shall be audited at the close 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 authorized by him in this behalf may require for the purpose of audit.

(4) Copies of the Auditor-General's report on the accounts shall be provided to the Commission and the Federal Government and shall also be available for public inspection on the web site of the Commission.

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

43 CO-OPERATION WITH INTERNATIONAL ORGANIZATIONS

The Commission may, subject to the prior approval of the Federal Government, co-operate with any foreign authority or international organization in the field of data protection / data security / data theft / unlawfully data transfer on the terms and conditions of any program or agreement for co-operation to which such authority or organization is a party, or pursuant to any other international agreement made or after the commencement of this Act.

CHAPTER VII

COMPLAINT AND OFFENCES

44 UNLAWFUL PROCESSING OF PERSONAL DATA

44.1 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 up to fifteen million rupees and in case of a subsequent unlawful processing of personal data, the fine may be raised up to twenty-five million,

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

45 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 up to five million rupees.

46 ISSUE ENFORMENT ORDERS AND IMPOSE PENALITIES

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 up to two point five million rupees.

(1) Where a Data Controller and/or Data Processor contravenes any provision of this Act or the rules or regulations made thereunder or policy issued by the Federal Government, or any direction issued by the Commission or condition of the registration, the Commission may by a written notice require Data Controller and/or Data Processor within fifteen days as to why an enforcement order may not be issued.

(2) The notice referred to in sub-section (1) shall specify the nature of the contravention and the steps to be taken by the licensee to remedy the contravention.

(3) Where anyone fails to:-

(a) respond to the notice referred to in sub-section (1); or

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

(c) remedy the contravention within the time allowed by the Commission, may, by an order in writing and giving reasons:-

i. levy fine which may extend to two hundred and fifty million rupees; or
ii. suspend or terminate the registration and impose additional conditions.

47 CORPORATE LIABILITY

A legal 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 legal person shall be punished with fine not exceeding 1% of its annual gross revenue in Pakistan or thirty million rupees, whichever is higher.

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

48 COMPLAINT

48.1 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, 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.

48.2 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.

48.3 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.

48.4 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.

48.5 After receipt of the complaint, the Commission may,

a) seek explanation from the data controller or data processor, after initial evaluation, 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.

48.6 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.

48.7 In case of failure of the data controller 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.

49 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 the purpose in the manner prescribed by the High Court for filing the first appeal before that Court or the Tribunal and the Court or the Tribunal shall decide such appeal within ninety days.

(2) A person aggrieved by any decision or order of any officer of the Commission acting under the delegated powers of the Commission may, within thirty days of the receipt

of the decision or order, appeal to the Commission in prescribed manner and the Commission shall decide such appeal within thirty days.

CHAPTER VIII

MISCELLANEOUS

50 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.

51 POWER TO MAKE RULES

51.1 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.

51.2 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.

51.3 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.

52 POWER TO MAKE REGULATIONS

The Commission shall issue regulations for exercising its powers and performance of its functions, for its internal working, appointment, promotion, termination and terms and condition of its employees not inconsistent with the provisions of the Act or the rules, for carrying out of its functions under this Act.

53 RELATIONSHIP OF THE ACT WITH OTHER LAWS

The provisions of this Act shall have effect notwithstanding anything to the contrary contained

in any other law on the subject for the time being in force. The articles of this Act will serve as bare minimum provisions and wherever there is any other applicable law on the subject, the provisions that have stringent effect will prevail.

54 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.

55 WINDING UP OF THE COMMISSION

No provision of any law relating to winding up of bodies corporate shall apply to the Commission. The Commission shall only be wound up by the law to be enacted by the Parliament for winding up of the Commission.