ELECTRONIC DATA PROTECTION AND SAFETY ACT 2005

An Act to provide for protection and safety to electronic data with regard to the processing of electronic data in Pakistan

Whereas it is expedient to provide for the processing of electronic data while respecting the rights, freedom and dignity of natural and legal 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) This Act may be called the Electronic Data Protection and Safety Act 2005.

(2) It extends to the whole of Pakistan and shall apply to the processing of electronic data which is collected or takes place within Pakistan, regardless of the location of the data processor or data controller.

(3) It shall come into force at once.

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

(a) “blocking”, means the storage of electronic data while any other data processing operation is temporarily suspended;

(b) “Certification Council”, means the Electronic Accreditation Certification Council established under the Electronic Transactions Ordinance 2002;

(c) “corporate data”, means any information relating to or owned by any person including financial, legal, business and processes;

(d) “data controller”, means the individual or person, who determines the purposes and means of the processing of electronic data, including security issues;

(e) “data filing system”, means any set of data structured according to several specific criteria suitable to ease their processing, composed of one or more units, in one or more physical locations;
(f) “data operator”, means an individual employed by data processor for the processing of electronic data;

(g) “data processor”, means the individual or person, who processes electronic data on behalf of a data controller;

(h) “data subject”, means the individual or person to whom the electronic data are related;

(i) “disclosure”, means the act of making electronic data known to one or more specified individual or person, excluding the data subject himself, by any means;

(j) “dissemination”, means the act of making electronic data known to unspecified individuals or persons, by any means;

(k) “electronic data” includes personal, corporate, foreign and local data;

(l) “foreign data” means both personal and corporate data collected outside Pakistan and sent to Pakistan for processing purpose only;

(m) “individual” means natural person;

(n) “local data” means both personal and corporate data collected within Pakistan for processing within or outside Pakistan;

(o) “person” includes an authority, trust, waqf, association, statutory body, firm, company including joint venture or consortium, or any other entity whether registered or not;

(p) “personal data”, means any information relating to an individual, identified or identifiable, directly or indirectly by reference to any other information;

(q) “processing”, means any operation or set of operations, whether or not performed by an information system, which involves collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, blocking, disclosure by transmission, dissemination, erasure or destruction of the data;

(r) “prescribed” means prescribed by rules or regulations made under this Act;

(s) “Regulations” means regulations made under this Act;

(t) “Rules” means rules made under this Act; and

(u) “sensitive data” means data 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, or provide information as to the health or sexual life of an individual and financial, or proprietary confidential corporate data;

3. **Manual and personal data.**— (1) The processing of personal or corporate data which are not performed by any information system or other automated means shall not be subject to the provisions of this Act unless the manual data is collected for the purpose of converting it into electronic data.

(2) The processing of personal data by an individual in the course of a purely personal activity or household and family purposes shall not be subject to the provisions of this Act, provided that the personal data are not intended to be systematically disclosed or to be disseminated.

4. **Government activity and exemptions.**— (1) This Act does not apply to the processing of personal or corporate data carried out by federal, provincial or local government.

(2) The federal government, in respect of local data only, by notification in the official gazette, may exempt any public or private sector, entity or business from the operation of this Act.

**CHAPTER II**

**PROCESSING OF FOREIGN DATA**

5. **Notice by data controller.**— (1) Data controller who wishes to perform processing of foreign data in Pakistan, which falls within the scope of this Act may at its option notify the Certification Council of his intention.

(2) If the data controller wishes to notify the Certification Council, he shall submit a notice to the Certification Council in a prescribed manner before the actual processing begins, regardless of the number of operations to be performed, or of the length of the data processing itself, for any number of processing with related purposes. A new notice is required only when any of the items specified in sub-section (3) changes, and shall be submitted before the change takes place.

(3) The notice referred to in sub-section (2) may include:

(a) name or trade name and address of the data controller and data processor;

(b) purposes and means of the processing;
(c) description of the data, the location where they are kept and the categories of data subjects to whom they relate;

(d) limits of data disclosure and dissemination;

(e) intended further transfers of data to any other country or territory outside Pakistan;

(f) general description that allows an assessment of the technical and organizational measures taken to ensure data security;

(g) specification of any data filing system which the processing is related to, and the connections, if any, with other data processing or data filing systems, whether within Pakistan or not;

(h) copy of the contract between data controller and data processor;

(i) the capacity and authority of the individual submitting the notice.

6. **Data processor.**— (1) The processor shall perform the data processing according to the lawful instructions received from the data controller. The data controller shall ensure at all times the strictest compliance with his instructions and provisions of this Act, and may do periodical verifications for this purpose.

(2) If necessary for organizational reasons, more than one data processor may be designated depending on the specific duties of the data processors. In case of more than one data processor the duties of each data processor shall be expressly defined in writing by the data controller.

(3) Data operators in charge of data processing shall act on the foreign data to which they have access only according to the instructions of the data controller or data processor.

7. **Processing.**— Foreign data that are subject to processing shall be:

(a) processed fairly and lawfully;

(b) stored for specified, explicit and lawful purposes;

(c) accurate and, when necessary, kept up to date;

(d) adequate, relevant and not excessive in relation to the purposes for which it is processed; and

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was processed.
CHAPTER III
COLLECTION AND PROCESSING OF LOCAL DATA

8. **Notice by data controller.**— (1) Data controller who wishes to collect and get processing of local data in Pakistan, which falls within the scope of this Act may at its option notify the Certification Council of his intention.

(2) If the data controller wishes to notify the Certification Council, he shall submit a notice to the Certification Council in a prescribed manner before the actual processing begins, regardless of the number of operations to be performed, or of the length of the data processing itself, for any number of processing with related purposes. A new notice is required only when any of the items specified in sub-section (3) changes, and shall be submitted before the change takes place.

(3) The notice referred to in sub-section (2) may include:

   (a) name or trade name, and address of the data controller and data processor;

   (b) manner of collection of local data;

   (c) purposes and means of the processing;

   (c) description of the data, the location where they are kept and the categories of data subjects to whom they relate;

   (d) limits of data disclosure and dissemination;

   (e) intended transfers of data to any country or territory outside Pakistan;

   (f) general description that allows an assessment of the technical and organizational measures taken to ensure data security;

   (g) specification of any data filing system which the processing is related to, and the connections, if any, with other data processing or data filing systems, whether within Pakistan or not;

   (h) copy of the contract between data controller and data processor;

   (i) the capacity and authority of the individual submitting the notice.

(4) The data controllers, who are members of any chamber of commerce, trade association and professional body recognized by any law may submit the notice through those organizations.
9. **Collection of electronic data.** (1) Electronic data that are subject to data processing shall be:

(a) processed fairly and lawfully;

(b) collected and stored for specified, explicit and lawful purposes;

(c) accurate and, when necessary, kept up to date;

(d) adequate, relevant and not excessive in relation to the purposes for which it is collected or processed;

(e) processed in accordance with the rights of the data subject; and

(f) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

10. **Information to data subject.**— (1) Data subject, any other individual or person from whom the local data is collected shall be given, prior to the collection and in writing, the following information:

(a) the purposes and means of the processing;

(b) whether replies to the questions are obligatory or voluntary;

(c) the possible consequences of failure to reply;

(d) the recipients or categories of recipients to whom data may be disclosed, and the limit of data dissemination;

(e) the existence of his rights; and

(f) the name or trade name, and the address of the data controller and, when designated, of the data processor.

(2) Some or all of the information described in Sub-section 1 may be omitted when it is already known to the person from whom the data is collected.

(3) Where the data have not been obtained from the data subject, the information described in Sub-section 1 shall be provided to the data subject at the time of undertaking the recording of the personal data or, if a disclosure is intended, no later than the time when the data is first disclosed.

(4) The provision of Sub-section 3 shall not apply when providing the information to the data subject would require an act declared by the Certification Council as clearly
disproportionate with respect to the protected right or, in the Certification Council's judgment, impossible, nor when the processing is required under an obligation by national, provincial or local laws.

(5) The Certification Council shall not question the compliance of the principles mentioned above unless a complaint is received from any data subject, data operator or employee of the data controller or data processor that the provisions of section 9 and 10 are being violated.

11. **Data processor.**— (1) The processor shall perform the data processing according to the lawful instructions received from the data controller. The data controller shall ensure at all times the strictest compliance with his instructions and provisions of this Act, and may do periodical verifications for this purpose.

(2) If necessary for organizational reasons, more than one data processor may be designated depending on the specific duties of the data processors. In case of more than one data processor the duties of each data processor shall be expressly defined in writing by the data controller.

(3) Data operators in charge of data processing shall act on the local data to which they have access only according to the instructions of the data controller or data processor.

12. **Processing.**— Local data that are subject to processing shall be:

(a) processed fairly and lawfully;

(b) stored for specified, explicit and lawful purposes;

(c) accurate and, when necessary, kept up to date;

(d) adequate, relevant and not excessive in relation to the purposes for which it is processed; and

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was processed.

**CHAPTER IV**

**DATA SUBJECT'S RIGHTS**

13. **Consent.**— (1) It would be the sole responsibility of the data controller to obtain the consent of the data subject, if required, who’s foreign or local data shall be processed within Pakistan.
14. Rights of foreign Data Subjects.— (1) Data subjects shall have all their rights, if any provided under the laws of the country or territory where the foreign data has been collected or data subject resides, only against data controller including confirmation as to existence of, access to, updating or rectification of their foreign data and objection to any or all operations involving the processing of foreign data and its intended purpose and will not deal directly with the data processor within Pakistan unless otherwise agreed between the data controller and data processor.

(2) The contract between data controller and data processor referred to in sub-section (1), if reduced into writing shall be filed with Certification Council within a period of three months of execution.

15. Rights of local Data Subjects.— (1) Data subjects shall have the right to ensure compliance of the provisions of sections 9 and 10, only against data controller including confirmation as to existence of, access to, updating or rectification of their local data and objection to any or all operations involving the processing of local data and its intended purpose and will not deal directly with the data processor within Pakistan unless otherwise agreed between the data controller and data processor.

(2) The contract between data controller and data processor referred to in sub-section (1), if reduced into writing shall be filed with Certification Council within a period of three months of execution.

(3) The Certification Council may prescribe the rights of the data subjects, limitations on the rights, manner of exercising those rights.

CHAPTER V

ELECTRONIC DATA SECURITY

16. Electronic data security.— (1) Electronic data that is subject to data processing shall be kept under custody and controlled in such a way as to minimize the risks of its destruction or loss, even accidental, of unauthorized access, unlawful processing or processing for other purposes than those for which the electronic data were collected, by means of appropriate precautionary security measures, having regard to the state of the art, the nature of the data to be protected and the peculiarities of the data processing itself.

(2) The minimal precautionary security measures shall be prescribed by the Certification Council through model regulations, within ninety days from the coming into force of this Act.
(3) The regulations described in sub-section (2) shall be reviewed and updated at least after every two years considering the technical advances and acquired experience after consulting the data processors.

17. **End of data processing.**— (1) Before ending the processing of electronic data, for any reason, the data processor shall notify the Certification Council of its fate in a prescribed manner, unless he is exempted by his data collector.

(2) The electronic data can be:

   (a) destroyed;

   (b) returned to data controller; or

   (c) stored for a purely personal activity and not intended to be systematically disclosed or to be disseminated.

18. **Damage caused by processing.**— Any data processor or data operator who willfully causes damage to the electronic data as a consequence of the processing in an improper way or not in accordance with the instructions of the data controller shall be bound to pay compensation determined by the Certification Council to the affected data controller.

**CHAPTER VI**

**DISCLOSURE AND DISSEMINATION**

19. **Data operators.**— The act of making electronic data known to data operators appointed by the data processor, in writing, to perform the operations related to the processing, and acting directly on his behalf, shall not be considered disclosure and dissemination subject to such limitation as may be agreed upon between data controller and data processor.

20. **Data disclosure.**— The disclosure and dissemination of personal or corporate data shall be permitted:

   (a) when the data controller has explicitly given his consent;

   (b) when it is performed under an obligation by national, provincial or local laws;

   (c) when necessary for the establishment, exercise or defence of legal claims in court; and

   (d) when requested by any government authority, defence forces and law enforcement agencies for purposes of national security or the prevention, investigation, detection and prosecution of criminal activities.
21. **Restrictions on disclosure.**— (1) The disclosure and dissemination of personal or corporate data for purposes different from those stated in the contract between the data controller and data processor and in this Act shall be prohibited.

(2) The Certification Council may forbid the dissemination of any or all electronic data related to a data subject or to a category of data subjects when such dissemination would conflict with a substantial public interest.

22. **Sensitive data.**— (1) The processing of Sensitive Data shall be conducted in such a way as to minimize the risks of unauthorized access or use, by means of appropriate precautionary security measures.

(2) The minimal precautionary security measures for the sensitive data shall be prescribed by the Certification Council through model regulations, within ninety days from the coming into force of this Act.

(3) The regulations described in sub-section (2) shall be reviewed and updated at least after every two years considering the technical advances and acquired experience after consulting the data processors.

23. **Transfer of foreign data.**— Transfer of foreign data to a country other than the country of its origin, in any form and with any means, even if temporary, shall be subject to the contract between the data controller and data processor.

24. **Transfer of local data abroad.**— (1) Transfer of local data to a country or territory not having adequate protection for the protection and safety of electronic data shall not be carried out without the permission in writing of the Certification Council.

(2) The Certification Council while granting permission mentioned in sub-section (1) in its discretion may impose conditions, propose appropriate measures and ensure compliance of such conditions and measures.

**CHAPTER VII**

**CERTIFICATION COUNCIL**

25. **Powers and functions of Certification Council.**— (1) The Certification Council for the purpose of this Act shall have the following powers and functions to,—

(a) create and maintain a registry of all processing operations according to notices submitted to it;

(b) verify on complaint whether the data processing is carried on in accordance with law and in conformity with the contract between data controller and data processor;
(d) hear claims from data controllers, data processors or data subjects;

(e) pass appropriate orders on such claims;

(g) prepare and encourage the drawing up of suitable codes of conduct and ethics by certain categories;

(h) verify the compliance of such codes with applicable laws and regulations

(i) seek views of data controllers and data processors on any matter related to electronic data;

(i) contribute to the publicity and enforcement of such codes;

(l) interact and cooperate with bodies performing similar functions;

(m) set up or accredit bodies to audit the security measures of the data processors; and

(n) draw up a yearly report on its activities and the state of implementation of this Act. Such report shall be submitted to the Federal Government no later than September 31 of the financial year following the one to which it relates.

(2) The registry described in sub-section (1), clause (a) shall be maintained according to the procedure described in the regulations.

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

26. Investigative powers.— (1) To perform its functions, the Certification Council may require any information and documents from any data controller, data processor, data operator, data subject or any third person.

(2) For the purposes of verifying the compliance with the applicable data processing provisions, the Certification Council may require access to data filing systems and other inspections and verifications where the processing is carried on, or wherever it is necessary to acquire useful information.

(3) The investigations on the data processing shall be carried on by any authorized official of the Certification Council or an accredited body for the purpose. If the data processing is found to be in violation of the provisions of this Act or any rules or regulations made thereunder or contractual arrangement between Data Controller and Data Processor, the Certification Council may require the data processor to comply with such provisions. If the investigation was requested by any data controller or data subject, the Certification Council shall inform him about the outcome of the investigation unless such information is not to be disclosed in the interest of national security.
(4) The Certification Council may request, if needed, assistance from other public and law enforcement authorities.

27. **Recruitment of employees, etc.**— (1) The Certification Council may, from time to time, appoint such officers, employees, consultants and advisers as it may consider necessary for the efficient performance of its powers and functions under this Act on such terms and conditions as may be described in the regulations.

(2) The Certification Council shall make regulations for recruitment of its employees.

(3) All members, employees, advisors and consultants of the Certification Council Members shall be subject to a duty of secrecy on any information on electronic data, data filing systems and processing operations to which they have had access in the course of their duties.

28. **Funds of Certification Council.**— The funds of the Certification Council for the purposes of this Act shall comprise of:

(a) grants from the Federal Government;

(b) fees collected from data controllers, data processors, complainants or others; and

(c) fines.

CHAPTER VIII

COMPLAINT AND OFFENCES

29. **Complaint.**— (1) Any data controller may lodge a complaint in a prescribed manner to the Certification Council if he does not feel satisfied with any action, contractual or otherwise, of his data processor.

(2) In case of local data any data subject or person having interest in the electronic data may lodge a complaint against any data controller in a prescribed manner to the Certification Council for enforcement of his rights or interest under this Act or any other law or contract.

(3) During the course of the investigation of the complaint mentioned in sub-sections (1) and (2), the complainant, data controller and data processor shall have the right to be heard by the Certification Council.

(4) After collecting all the necessary information the Certification Council shall, if the complaint is found to be correct, order the data processor or data controller to refrain from his unlawful or undesirable behaviour, impose fine not exceeding one million
rupees or order appropriate measures to protect the electronic data and the rights and interest of the complainant.

(5) During the pendency of the investigation the Certification Council may temporarily order the blocking of some or all of the electronic data, or impose a ban on any or all the operations of processing.

(6) Any final order of the Certification Council may be appealed against by any aggrieved individual or person as First Appeal against Order before the High Court having territorial jurisdiction, within thirty days from the communication of the said order.

30. **Unlawful processing of personal data.**— Anybody who, acting for his own or anybody else's benefit, processes electronic data in violation of any of the provisions of this Act or contract with the Data Controller, shall be punished with imprisonment for a term not exceeding three years or fine not exceeding three million rupees or both.

31. **Failure to adopt appropriate data security measures.**— Anybody 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 the regulations, if binding or contract between the data controller and data processor, shall be punished with imprisonment for a term not exceeding three years or fine not exceeding three million rupees or both.

32. **Failure to comply with orders.**— Anybody who fails to comply with the orders of the Certification Council when he is required to do so, shall be punished with imprisonment with imprisonment for a term not exceeding three months or fine not exceeding one hundred thousand rupees or both.

33. **Exception.**— Notwithstanding anything contained in this chapter, Act or any contract between the parties, shall constitute an offence if any data operator, employee of data controller or data processor acts on reasonable ground and in good faith to inform the Certification Council of any perceived violations of the Act, rules, regulations and contract between the data controller and data processor. On the request of the informer the Certification Council shall maintain secrecy about his identity in any or all circumstances.

34. **Corporate liability.**— A person shall be held liable for a criminal offence committed on his instructions or for his benefit or lack of required supervision by any individual, acting either individually or as part of an organ of the person, 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 ten million rupees.
Provided that such punishment shall not absolve the criminal liability of the individual, who has committed the offence.

35. **Offences to be bail-able, compoundable and non-cognizable.**— (1) All offences under this Ordinance shall be bail-able, compoundable and non-cognizable.

(2) The prosecution of the offence under this Act shall only be initiated by the Certification Council.

36. **Prosecution and trial of offences.**—No Court inferior to the Court of Sessions shall try any offence under this Act.

**CHAPTER IX**

**TEMPORARY AND MISC PROVISIONS**

37. **Temporary provisions.**— (1) All data processors shall adopt necessary security measures within six months from the day in which the regulations, if binding, on the subject come into force. In the meantime, electronic data should be kept under custody in such a way as to prevent any increase of the risks to the electronic data.

(2) In case of local data the data controller shall comply with the principles laid down in section 9 and 10 of this Act within a period of one year.

38. **Other Laws.**— For the purposes of Electronic Crimes Act 2005, any electronic or information system containing electronic data shall be considered as sensitive electronic system.

39. **Power to make rules.**— The Federal Government may, by notification in the official Gazette, make rules to carry out the purposes of this Act.

40. **Power to make regulations.**— The Certification Council may make regulations to carry out the purpose of this Act.