ELECTRONIC DATA PROTECTION ACT 2005

An Act to provide for protection 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 commencemen**t.—(1) This Act may be called the Electronic Data Protection 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) "corporate data", means any information relating to or owned by any person including financial, legal and business processes;

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

(d) "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;

(e) "data operator", means an individual employed by data processor for the processing of electronic data;

(f) "data processor", means the individual or person, who processes electronic data on behalf of a data controller;

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

(h) “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;

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

(j) “electronic data” means any information which is being processed by means of any information system, is recorded with the intention that it should be processed by means of such information system, or is recorded as part of a relevant data filing system or with the intention that it should form part of a relevant data filing system and includes personal, corporate, foreign and local data;

Explanation.—The words “information” and “information system” used in sub-clause (k) shall have the same meaning as defined in the Electronic Transaction Ordinance 2002 (LI of 2002);

(k) “federal government” means the federal government of Pakistan;

(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, use, alignment or combination, blocking, disclosure by transmission, dissemination, erasure or destruction of the data;

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

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

(t) "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 AND LOCAL DATA

5. **Data processor and data operators**.— (1) The data processor shall perform the data processing in the prescribed manner and according to the instructions received from the data controller unless it contravenes any law.

(2) Data operators shall act on the foreign or local data, as the case may be, to which they have access only according to the instructions of the data processor.

6. **Processing**.— Processing of foreign or local data, as the case may be, shall be:

(a) done fairly and lawfully; and

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

7. **Collection of local data** — Local data that are subject to data processing shall be:

(a) collected with due diligence, fairly and lawfully;

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

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

(d) processed in accordance with the rights of the data subject and, when necessary, kept up to date.

8. **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, if 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.

CHAPTER III

DATA SUBJECT'S RIGHTS

9. **Consent**.— It would be the sole responsibility of the data controller to obtain the consent of the data subject, if required, whose electronic data shall be processed within Pakistan.

10. **Rights of foreign Data Subjects.**— 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.

CHAPTER IV

ELECTRONIC DATA SECURITY

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

(2) The minimal precautionary security measures shall be as prescribed.

12. **End of data processing** — (1) Before ending the processing of electronic data, for any reason, the data processor shall notify the data controller of its fate.

(2) The electronic data can be:

(a) destroyed; or

(b) returned to data controller.

CHAPTER V

DISCLOSURE AND DISSEMINATION

13. **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.

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

(a) by the data processor, when the data controller has explicitly given his consent or as provided in the contract with data controller;

(b) by data controller or data processor,—

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

(ii) when necessary for the establishment, exercise or defense of legal claims in court;

(iii) when requested by any relevant government authority for purposes of national security or prevention, investigation, detection and prosecution of criminal activities; and

(iv) as may be prescribed.

15. **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 as prescribed.

16. **Transfer of local data abroad**.— Transfer of local data to any territory outside Pakistan shall only be carried out in the prescribed manner.

CHAPTER VI

FEDERAL GOVENMENT

17. **Powers and functions of federal government** — (1) The federal government shall have the following powers and functions to,—

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

(b) verify the compliance of such codes with applicable laws;

(c) seek views of data controllers and data processors on any matter 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 processors.

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

CHAPTER VII

COMPLAINT AND OFFENCES

18. **Complaint**.— (1) Any data controller may lodge a complaint in a prescribed manner to the Sessions Judge [*may be changed with ICT tribunal, if created*] having territorial jurisdiction, 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 Sessions Judge, having territorial jurisdiction, for enforcement of his rights or interest under this Act or any other law or contract.

(3) The Sessions Judge, if feels necessary, may direct any person or individual to investigate into the complaint lodge before him and report back to the court. To perform his functions, the person or individual so directed by the Sessions Judge, may require any information and documents from any data controller, data processor, data operator, data subject or any third person and if further authorized, may require access to data filing systems and where the processing is being carried on.

(4) 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.

(5) After collecting all the necessary evidence the Sessions Judge 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, the rights and interest of the complainant and ensure compliance of the applicable provisions of this Act, rules and the contract.

(6) During the pendency of the investigation the Sessions Judge 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.

(7) The Sessions Judge may request, if needed, assistance from any public and law enforcement authorities.

(8) Any final order of the Sessions Judge 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.

19. **Unlawful processing of electronic 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 or Data Processor, as the case

may be, shall be punished with imprisonment for a term not exceeding three years or fine not exceeding three million rupees or both.

20. **Unlawful dissemination and disclosure**.— Anybody who, acting for his own or anybody else's benefit, disseminate or disclose electronic data in violation of any of the provisions of this Act or contract with the Data Controller or Data Processor, as the case may be, shall be punished with imprisonment for a term not exceeding three years or fine or both.

21. **Sensitive Data** — In case the offence committed under section 19 and 20 relates to Sensitive Data the maximum term of punishment shall be five years.

22. **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 rules, 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 or both.

23. **Failure to comply with orders**.— Anybody who fails to comply with the orders of the Sessions Judge when he is required to do so, shall be punished with imprisonment with imprisonment for a term not exceeding three months or fine or both.

24. **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 Sessions Judge of any perceived violations of the Act, rules and contract between the data controller and data processor. On the request of the informer the Sessions Judge shall maintain secrecy about his identity in any or all circumstances.

25. **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.

26. **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 with the prior of the authorized officer of the federal government.

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

CHAPTER VIII

TEMPORARY AND MISC PROVISIONS

28. **Temporary provisions**.— (1) All data processors shall adopt necessary security measures within six months from the day in which the rules, 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 sections 7 and 8 of this Act within a period of one year.

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

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