Electronic Data Protection in پاکستان

| Electronic Data Protection in Pakistan:

What Needs to be Done? |

A Bytes for All, Pakistan report in collaboration with Association for Progressive Communications and Privacy International | November 2017

Acknowledgments

Authors: Umer Gilani, Haroon Baloch, Shaheera Jalil Albasit, Furhan Hussain
Editors: Jo Antoniewska, Tehmina Zafar
Design and Layout: Nida Meyer Mian

We would also thank Association for Progressive Communications (APC) and Privacy International (PI), European Union (EU) and International Development Research Centre (IDRC) for their collaboration and support without which this paper would not have been possible.

Bytes for All, Pakistan

TABLE OF CONTENTS

ABOUT THIS REPORT

The increased digital access in human lives has facilitated its work and appended additional spaces to the existing ones. Knowledge is no more inaccessible or confined to books, rather it has been taken to virtual spaces. Pakistan is relatively a new to this advancement, however, there has been a meticulous debate in progress to regulate these spaces and counter the crimes facilitated by the internet. The new laws are being introduced to fight back the technology driven crimes, however, various provisions have enabled the State to curb on fundamental freedoms. On the other hand, the government also began employing the sophisticated technology to collect citizens' information through digital means and store it as the State's repositories.

These repositories form a massive database that contain personal information of citizens including biometric prints of millions of people, which the government also claims is one of the world's largest databases. Mass collection of citizens' digital data raises questions vis-à-vis security and protection of the data, and sharing with other parties, foreign governments, agencies, as well as corporate entities. The government of Pakistan has always been reluctant to answer these questions and uncover the information of public interest in the guise of national security.

This background paper will explore the data protection aspect of existing state of privacy in Pakistan in order to strike a debate about its urgency and need.

Background

The advances in digital technology and the birth of internet have revolutionised the way people communicate, perform day-to-day activities, gain knowledge and access information. Knowledge is no longer the privilege of the few. Rather, it is increasingly available to the ordinary people through various freely available digital platforms and spaces. Although Pakistan is relatively new to these technological advancements, there has been an ongoing debate here about how to best regulate such digital platforms and spaces, and how to counter the increasing criminal activity that the internet facilitates.

Although various legislation has been introduced over the years in order to prevent the technology driven crime, the ambiguity of its provisions has unfortunately also given the State carte blanche for breaching the fundamental rights and freedoms of its citizens. Moreover, the Pakistan's government also began employing sophisticated digital technology to bulk collect and store citizens' personal data in its repositories. These repositories form an enormous database of personal information, including biometric data of millions of people, claimed by the government to be one of the world's largest.

Understandably, such bulk collection of personal information raises questions about the state of security of such repositories, and whether or not the data collected is shared with third parties or other foreign governments. The government of Pakistan has so far been extremely reluctant to answer any questions about any personal data it holds or shares, stating national security reasons. This background paper explores the state of privacy in Pakistan and the data protection aspects of Pakistan's privacy law. Its purpose is to start a debate about the pressing need to introduce new data protection legislation into Pakistan's domestic law.

Data, Big Data and Data Protection

Data protection is a term describing the body of rules that governs the collection and processing personal information ('data') about a living identifiable person ('data subject'). Data is processed, meaning 'collected, stored and shared, by a legal entity ('data controller' or 'data processor') and is protected through the creation and implementation of law.[1] The existence of well-established legal data protection framework gives citizens the right to make requests about what data is held about them, how and when it is collected, stored and whether or not it is shared with other individuals or entities ('third parties'). More importantly, such legal framework, if properly implemented, provides people with the power of consent, meaning the ability to give or withdraw their permission for processing of personal data.

Data can be used for various purposes, including decision making, reasoning or calculations[2] and can become a valuable commodity to those who may wish to market their products or services back its owners.

Data protection legislation can be extremely difficult to draft and implement, especially when other means that negate or violate the concept of data protection, already exist in law. It is, therefore, very important to begin educating citizens right now about the importance and value of their data, and more importantly, why it must be protected at all times.

People should understand that the knowledge of one's past behavior can give an accurate prediction of their future actions and therefore, the likelihood of them buying what others want to sell to them.[3] This not only makes the data controllers extremely knowledgeable, but also wealthier and more powerful.

Moreover, it is important to note that it is not only the corporate business entities that are keen to own personal data. External governments, domestic law enforcement agencies, and even criminal organisations, to name a few, can also benefit immensely by studying it.

1. *Privacy International. What is Data Protection. https://www.privacyinternational.org/node/44*
2. *Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/data*
3. *Privacy International. Data Protection. https://www.privacyinternational.org/node/570*

Big data sets of human behavior, often called big data, can become important pieces of intelligence that may be used to help spot behavioral patterns. This in turn can be used to help reduce the effects of natural catastrophes and beat diseases. However, the same data in the wrong hands can be used in a way to harm others. This is why it is essential to expand this debate towards the need to more effectively oversee all data processing activities, and implement strong and effective data protection laws. Only this will ensure that one's privacy, a constitutional and universal human right, is not unfairly violated.[4]

Data Protection Law in Pakistan – Need of the Day

Pakistan's data territory has never been in a more urgent need of institutionalized regulatory structures for data protection. The draft Data Protection Act which was introduced in 2005[5] was not drafted following an exhaustive, far-reaching, all-inclusive multi-stakeholder consultation which a proposition of data regulation of Pakistan's scale unarguably merits.[6]

The draft Act was not promulgated into law[7] and Pakistan's data-scape has continued to operate in the grave absence of data protection legislation.

No coordinated framework exists[8] at federal and provincial levels to determine and regulate how data flows occur within and through the country, and how data subjects, data controllers, and data processors interact with data which does and does not belong to them. There are thus no elaborate terms of legal compliance and accountability in practice,[9] under which data sharing by data collectors and processors including but not limited to telecommunication and internet service providers, e-businesses, financial institutions, and government services portals, is regulated.

Such an environment does not recognize the stakes of data subjects in the data cycle, and does not acknowledge the critical need for securities against data vulnerabilities like loss of confidentiality, unauthorized access, and breaches.

4. *Ibid.*
5. *Morrison Moerster. Electronic Data Protection Act 2005 [Draft]. http://media.mofo.com/docsmofoprivacy/PAKISTAN%20Draft%20Law%202nd%20Revision%20.pdf*
6. *Association for Progressive Communication. Blog: https://www.apc.org/en/blog/pakistan-electronic-data-protection-act-2005-final*
7. *Privacy International. https://www.privacyinternational.org/node/970*
8. *Ibid.*
9. *Graham Greenleaf. http://www2.austlii.edu.au/~graham/publications/2009/PLBI100_21years.pdf*

This also means that treatment of data by financial giants, businesses – big and small, and government repositories, for example those housing the citizen biometric database (NADRA)[10] and integrating the same with 24/7 public space CCTV surveillance (Safe City Projects), among others, is largely not threatened by any serious and lasting consequences of monetary sanctions and loss of public reputation in cases of data violation by them.[11] This is a rights perspective. And therefore, it is pragmatic to expect one such data protection legislation in Pakistan to be contextual - that is – also informed by purely business needs of the data capitalist.

Another example is the US government's SKYNET program which is used by the National Security Agency (NSA), also notorious for mass surveillance of people around the globe. In the case of SKYNET, a terrorist fighting program, a computer algorithm sifts through data of millions of people identifying habits and patterns which the coders of the algorithm arbitrarily decide as traits of terrorists. The program has been used to conduct hundreds of automated drone strikes on civilians in Pakistan and Afghanistan, out of which many individuals were feared to have nothing to do with terrorism.

So how did the US government get hold of such vast amount of data? While this is an important question, it is clear that this would have happened as a result of extremely weak data protection measures by those who were entrusted with this data - the government which collects and stores millions pieces of biometric identifiers of citizens, as well as the corporate telecommunications company that also collaborates with the government to ensure this data is centralized.

In her April statement, the Minister on Information Technology and Telecommunications (MoITT) said that she was concerned that big corporations would be a hurdle in the enforcement of data protection laws in the country[12]. While this is an important thing to consider, it is essential that the new set of laws covers all industry sectors and state functions. This includes data sharing with foreign governments which are not bound by local laws.

10. About us. NADRA. https://www.nadra.gov.pk/about-us/
11. Is NADRA keeping your biometric data safe? https://www.dawn.com/news/1290534
12. Ministry to introduce DPA within three months. https://www.pakistantoday.com.pk/2017/04/05/it-ministry-to-introduce-dpa-within-three-months/

Other technology solutions that NADRA also provides include, but are not limited to, security and surveillance. These are customizable solutions easy to deploy and configure, integrated with verification through its vast database, backed with multi-biometric features of fingerprints and facial, and are based on highly flexible, scalable and upgradable architecture for personnel access control, vehicle access control, intelligent video surveillance and safe cities[13].

The National Database and Registration Ordinance, 2000 lacks in providing elaborated security mechanisms to protect and restrict the misuse of citizens' data in possession with the authority. It also lacks in providing redressal mechanisms to victims of misuse of data. Moreover, the law gives indemnity to the Federal or the Provincial governments, Local Authority or any Registration Officer exercising any power and performing any function under this Ordinance, for anything which is in good faith. This indemnity encourages the State or its apparatus to misuse powers or citizens' data and it would be easy to interpret their actions taken as "in good faith"[14]. Bytes for All, Pakistan[15] has made multiple right to information ('RTI') requests to NADRA questioning their security protocols employed at their data centers to make these repositories secure, existing mechanisms in practice to share citizens' data with other national institutions and foreign governments, and third parties engaged to acquire technology used to build these repositories[16]. The objective of such requests was to open up public interest information so to hold the government accountable and ensure transparency in the dubious systems.]

Sensitive Data and Big Data Owners

Where personal data can divulge one's different behavioral patterns, it can also expose the information that a data subject would opt not to publicise, in order to avoid socio-economic impact on their life. Such information, called sensitive data[17], could, for example, include medical records stored by a health facility or an insurance company. The disclosure of such . if the data subject suffers from a serious illness the a disclosure of such sensitive data might result in a job loss as their employer might consider the illness to be a reason for reduced efficiency at work.

13. *Security and surveillance. NADRA. https://www.nadra.gov.pk/solutions/security-solutions/*
14. *The National Database and Registration Ordinance 2000. http://nasirlawsite.com/laws/nadra.htm*
15. *About us. Bytes for All, Pakistan. http://content.bytesforall.pk/about*
16. *Online record of B4A's RTI requests. http://rtirequests.pk/*
17. *Definition of sensitive data by ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/*

Moreover, the disclosure of personal data or its purpose may result in limitations to one's private life. Although, not all processing activities can be regarded as privacy breaches or limitations, if performed unlawfully or disproportionately, such activities may be treated as privacy breaches.

The example of NADRA's processing activities can illustrate the above. As NADRA holds biometric data of most of the Pakistani population, its use by a third party, such as the Election Commission of Pakistan, for preparation of electronic rolls, or for verification purposes by the Federal Investigation Agency on the directions of a court in a criminal case, will not be considered as a breach of privacy. That is because such activities are performed to either facilitate a legitimate procedure of the State, or to protect the society from a probable danger.

However, if personal is transferred without authorisation by the NADRA or its officials to a third party for economic or political reasons, such transfer would be considered as a breach and violation of the citizen's human rights.

The Pakistan Telecommunications (Re-organization) Act, 1996

The Pakistan Telecommunications (Re-organisation) Act 1996 ('PTA') was passed in order to govern telecommunications industries, after introduction of mobile services and the internet. However, PTA provided unnecessary powers to the government to stifle freedom of expression and violate right to privacy of citizens. Major concerns vis-a-vis right to privacy that have emerged since its promulgation are as follows:

- It authorizes the government to intercept digital communications by employing surveillance technologies;
- It restricts the use of encryption technology, not only to communicate securely but also to protect digital data and access the internet by by passing restrictions on certain content.

Section 54(1) of PTA provides that in the interest of national security or in the apprehension of any offense, the Federal Government may authorize the interception of communications. Furthermore, Section 57(2)(ah) authorizes the Federal Government to make rules on the interception of communications without setting any standards[18].

18. *Pakistan: Telecommunications (Re-organization) Act. Legal analysis by Article 19. https://www.article19.org/data/files/medialibrary/2949/12-02-02-pakistan.pdf*

1. No one shall be subjected to arbitrary or unlawful interference with privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

However, the language of Sections 54(1) and 57(2)(ah) does not fulfill the guidelines set under the ICCPR and principles of necessity and proportionality. The unlawful interference means that no interference can take place except in situations where the law contemplates it as necessary and reasonable after obtaining a warrant from a court stating probable cause or reasonable grounds.[19]

Interception of communication also limits human rights including freedom of expression, association and freedom of movement. Digital surveillance badly impacts free flow of information among individuals or groups by means of the internet. This also limits the ability of media, journalists, human rights defenders, and marginalized communities to operate freely and fearlessly because keeping certain information, data and sources confidential and anonymizing their identity are key for their work and preventing from being victimized by state and non-state actors[20]. In 2013 report, former UN Special Rapporteur Frank La Rue stated:

"... undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions on anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization."

19. *Pakistan: Telecommunications (Re-organization) Act. Legal analysis by Article 19. https://www.article19.org/data/files/medialibrary/2949/12-02-02-pakistan.pdf*
20. *United Nations Human Rights Committee, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), CCPR/C/GC/16, 4 August 1988 http://ccprcentre.org/page/view/general_comments/27798*

Several provisions in PTA Act also put bar on encryption and the ability of users to be able to communicate anonymously by using Virtual Private Networks ('VPN'). VPNs bypass all monitoring mechanisms enabled by the government and the users can access any information without disclosing their identity. ISPs and telecommunication companies have strict directions to comply with its orders with regard to prohibition of usage of all such mechanisms including encrypted VPNs, which conceal communication to the extent that prohibits monitoring[21].

Section 5(2)(b) was used as justification for the "Monitoring and Reconciliation of Telephony Traffic Regulations, 2010" and July 21, 2011 Directive ordering ISPs and mobile phone companies to block users from using VPNs to access the internet. Freedom of expression and right to privacy are at stake in the presence of these mechanisms which enable excessive blocking and filtering of legitimate content, and the interception of communications.[22]

The Prevention of Electronic Crimes Act (PECA), 2016

In August 2016, the government promulgated the Prevention of Electronic Crimes Act ('PECA'), 2016, which contains many provisions related to digital data and suggests heightened punishments (Appendix 2). These provisions are related to unauthorized access to digital information or information system, critical infrastructure, electronic forgery, unauthorized interception or use of identity information, etc. In many procedural sections of the Act, unabated and unnecessary powers are conferred upon law enforcement agencies (LEAs). These include but are not limited to search and seizure of digital devices, gadgets and private data, expedited presentation and acquisition of data, retention of traffic data, disclosure of content data, confidentiality of data, and international cooperation.

The provision on expedited presentation and acquisition of data, Section 31, permits the Authorized officer to take the custody of private data stored in an information system without seeking prior Court permission for such.

21. PTA Notification: Usage of Encrypted VPNs (original letter). http://twitpic.com/5woaka
22. Pakistan: Telecommunications (Re-organization) Act. Legal analysis by Article 19. https://www.article19.org/data/files/medialibrary/2949/12-02-02-pakistan.pdf

The Authorized officer is also granted the discretion of keeping the data for 24 hours without any seizure orders from the Court. This provision grants unnecessary authority to the Authorized officer, who during the custody of specific data can modify or make changes to it, which later can be used as an electronic evidence against the owner of the data.

Section 32 of the Act makes it binding for all Internet Service Providers (ISPs) and Online Service Providers (OSPs) to retain traffic data of all subscribers for a period of one-year. This time period is by no means justifiable and according to global standards. Similar provisions had also been introduced in some European states. The Grand Chamber of the European Court of Justice (ECJ) had struck down the Directive No. 2006/24/EC[23] on Retention of Data. The ECJ declared the retention of data for one-year as invalid on the ground that European legislators had exceeded the limits of proportionality in forging the Directive[24]. In March 2015, a district court in the Netherlands also struck down the country's 2009 Telecommunication Data Retention Act (TDRA), which also required the telecommunication and Internet service providers to save the traffic and location data of subscriber for 12 months.

In Pakistan's context, this provision is also inappropriate because retention of sensitive data of citizens may lead to misuse of the data, especially when there are no transparent mechanisms on the data protections are available, or in case of misuse of the data or powers of the Authority, what platform will the seek justice.

Section 35(g) of PECA authorizes LEAs to access encrypted information in possession of any citizen who would be an alleged suspect of an offence. Moreover, section 15 restricts production, making, adapting, exporting or supplying of technologies which may be used to facilitate an offence. Such sections discourage software programmers and coders to produce and use of encryption enabled applications to secure digital data and information.

23. Directive 2006/24/EC of the European Parliament and of the Council. http://eur-lex.europa.eu/eli/dir/2006/24/oj
24. European Union: ECJ Invalidates Data Retention Directive. https://www.loc.gov/law/help/eu-data-retention-directive/eu.php

Use of technologies that enable encryption and anonymity are very important in digital age where mass surveillance is compromising the secrecy of information and personal data of citizens in general and of vulnerable communities in particular. In the context of Pakistan, such technologies are very relevant as well.

Section 42 of PECA is regarding cooperation with alien governments, agencies or international organizations in terms of sharing, collecting, preserving and transferring the digital data of Pakistan citizens or carry out real-time interception. Under this Section, the Federal Government has been given discretionary powers to share all these information, but no oversight mechanism is available within the law.

This section is highly controversial in the context of citizens' privacy. With the proven facts revealed in its report[25] by the Privacy International, the intentions of Section 42 are clear that the government is legitimizing all such practices where it was already sharing personal data and information of Pakistani citizens with foreign agencies running controversial surveillance programmes. "Pakistan has participated in and has been subject to, including programmes operated by the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ)": the report disclosed.

Intersection of PECA and Investigation for Fair Trial Act (IFTA)

PECA 2016 also provides justification for real-time collection and recording of infor-mation under Section 39. A set of concerns rises where it mentions the Authorized agency as notified under Investigation for Fair Trial Act, 2013 can intercept or carry our surveillance on communication of any person after getting permission from the Court[26]. According to Section 3 of IFTA 2013, the authorized agencies also include non-civilian intelligence agencies including the Inter-Services of Intelligence (ISI) and three Services Intelligence Agencies, which are intelligence wings of three armed forces.

25. Tipping the scales: Security and surveillance in Pakistan. (2015, July). Retrieved June 6, 2016, from https://www.privacyinternational.org/sites/default/files/PAKISTAN REPORT HIGH RES 20150721_0.pdf

26. Investigation for Fair Trial Act, 2013. www.na.gov.pk/uploads/documents/1361943916_947.pdf

The only civilian intelligence agency included in the list are the Intelligence Bureau and the Police. In Pakistan, it has been witnessed that questioning non-civilian intelligence agencies and holding them accountable for misuse of powers even by the higher courts is an uphill task[27].

Language of IFTA 2013 is very broad and employs subjective terms. It potentially vio-lates the internationally recognized principles of human rights, the Constitution and principles of natural justice.[28] IFTA allows that the Authorized intelligence agencies can seek surveillance warrants from the Court in a private hearing in chamber of the Judge against any individual without giving him or her a chance to present his or her opinion on the matter. Also the law lacks provision of any mechanism under which the individual subject to surveillance can challenge the issuance of warrants.

With all these apprehensions on IFTA 2013, Section 39 of the PECA can be problematic when it comes to accessing private data or information where another law legitimizes the collection and recording of information in real-time.

The Electronic Transaction Ordinance, 2002

Electronic Transaction Ordinance, 2002 does not regulate data protection directly. However, Section 36 criminalizes unlawful or unauthorized access to information, which in terms is another interpretation of right to privacy of digital data or electronic information. However, the argument is on the broadness and vagueness of the law. A lot of digital information stored in information systems or devices is of public interest and important for accountability and transparency. Journalists, researchers, and academicians get a hold of much of the digital data from unauthorized sources and publish is for public interest. Vague provisions like Section 36 create a space to criminalize such type of expression. A set of similar Sections (Sections 3 to 8) have also been replicated in PECA, 2016 with heightened punishments between three months to seven years, which have potential for criminalizing legitimate expression.

27. SC orders: ISI, MI granted more time to produce missing persons. https://tribune.com.pk/story/334795/sc-orders-isi-mi-granted-more-time-to-produce-missing-prisoners/
28. Unfair trial act. http://nation.com.pk/columns/19-Apr-2013/unfair-trial-act

Punjab Safe Cities Authority Act, 2016

Punjab Government has recently established Punjab Safe Cities Authority (PSCA) through a Governor order in 2015, which the Punjab Assembly approved in February 2016 as an Act[29]. The short preamble of the Act mentions the purpose of the Act as, "to establish Punjab Safe Cities Authority for purposes of construction, development and maintenance of city-wide integrated command, control and communications system in major cities of Punjab in order to ensure safety and security of the people, and for other purposes." This is very broad and open to any interpretation as it mentions that beside safety and security it also will be used for "other purposes".

Section 2 of the Act defines "ancillary facilities" that it includes the facilities and equip-ment provisioned or developed by the Authority including fences, cameras, poles, wir-ing, antennas, surveillance systems, control rooms, generators, lights, fans and other facilities. However, the Act itself is completely silent on mass surveillance mechanisms and data protection of the citizens.

Under Sections 18 and 19 of the Act, the Authority framed rules and regulations for the purpose of this Act, which are not public. Bytes for All, Pakistan got a hand to it by filing Right to Information request to the Authority . According to Section 3(1) of the Regula-tions, the PSCA will install ancillary facilities to monitor the City and to generate elec-tronic data which will be recorded and stored in the data center(s) of Integrated Com-mand and control Center (IC3). Whereas Section 3(2) says that a quantum of electronic data within the range of ancillary facility shall be generated to facilitate in the criminal cases. According to Section 3(3), all generated data in electronic form shall be preserved for up to seven years and made available in the data center. Mechanisms for protection of electronic data are again missing.

29. The Punjab Safe Cities Act 2016. http://punjablaws.gov.pk/laws/2619.html

The Telegraph Act,1885[30]

This British law was enacted in October 1885 in the Indian subcontinent by Imperial Legislative Council before partition to govern wired and wireless telegraphy, telephones, teletype, radio, visual, or electromagnetic communications. In Pakistan, this law is still in force and with respect to the right to privacy of wired or wireless communications, it Sections 19-A, 24, 25, 25-A, and 30 are of significance.

Section 19-A allows a person to legally damage telegraph or interfere with the tele-graphic communication subject to seeking permission from the telegraphic authority by submitting a written notice prior to commencing such act. However, any such exercise without seeking permission can be abstained by a Magistrate of first or second class on the application of the telegraphic authority. Here the word "person" is very subjective. Anyone can come under the definition of person, a law enforcement officer or an ordinary citizen. However, this Section is written in broad manner and can be problematic.

Section 24 is about learning the contents of telegraph message unlawfully. This Section punishes the perpetrator with imprisonment of up to one year.

Section 25 deals with intentional tampering or damaging with telegraphs and covers the acts of preventing or obstructing the transmission or delivery of any message, or intercepting or acquainting himself with the contents of the message, or committing mischief, shall be punishable with imprisonment for up to three years, or with fine or with both.

According to Section 25-A, if a person damages any telegraph line negligibly or will-fully, and by reason of this damage so caused interrupted, he or she will be punished with fine of up to one thousand rupees.

Section 30 deals with fraudulent retention of message in situations where a message is mistakenly delivered to a wrong person by the telegraph officer, or the recipient fraudulently retains such message, or wilfully secretes, shall be punished with imprisonment for up to two years with fine or both.

There is no legislation currently in force dealing specifically with data protection in Pakistan. However, various laws deal with the protection of confidential information and data in relation to specific areas. Some examples are:

- Qanun-e-Shahadat 1984 (Pakistani law of evidence) which provides for advo-cate-client confidentiality.
- The Electronic Transactions Ordinance 2002, which provides for confidentiality of information systems.
- Banking Companies Ordinance 1962, which provides for confidentiality of information with respect to customers of banks and financial institutions.

Electronic Data Protection Bill, 2005

i. Analysis of 'Electronic Data Protection Bill, 2005

Here, we shall present an analysis of the Electronic Data Protection Bill, 2005 in the light of:

a) International standards and guidelines;

b) Pakistan's international commitments and constitution; and

c) Relevant existing laws in Pakistan

d) Any other relevant resources.

Before proceeding to the text of the Electron Data Protection Bill, it is useful to cast a look at the existing provisions of Pakistani law which are related to data protection.

ii. A Summary of Existing Legal Provisions Related to Data Protection in Pakistan

At present, Pakistan does not have a specialized statute dealing with data protection. However, this does not mean that we live in a complete legal vacuum with regard to data privacy. To the contrary, there are both general and specific legal provisions of Pakistani law which relate to data privacy, either directly or indirectly.

A general concept of right to data privacy can be found latent in Pakistani constitutional law. Likewise, in various sectors of the life, especially in the areas of e-commerce and banking, spe-cific statutory provisions dealing with data protection can be found. These are discussed below.

iii) Constitutional Right to Privacy

The foremost provision relating to the general right to privacy is Article 14 of the Constitution of the Islamic Republic of Pakistan (hereinafter "the Constitution") which promises: "The dignity of man and, subject to law, the privacy of home, shall be inviolable.

Although the text of Article 14 refers to privacy "of home", the superior courts of Pakistan have, in countless judgments, interpreted this provision very expansively.[30] The prevailing interpretative approach of Pakistani courts towards this specific Article, and towards the Constitution in general, is not "textual"; it is "purposive" or "dynamic". The Courts do not restrict it to home-related privacy only. They have held that this Article was meant to protect a very broad notion of human privacy and therefore the right to privacy of personal data is very much included in its scope. By way of illustration, we may mention two concrete examples of the expansive interpretation of Article 14 fundamental right to privacy: In. M.D. Tahir Advocate vs. Director, State Bank of Pakistan and Others (2004 C L D 1680), the Lahore High Court clarified that an account holder's right to privacy of his banking data is part and parcel of his fundamental rights and this right cannot be abridged without good cause. Likewise, in Suo Moto Case of 1996 which concerned the phone tapping of Supreme Court judge, it was stated that a citizen's telephone conversations are protected by Article 14; they cannot be intercepted or monitored except when it is absolutely necessary and in a manner which is reasonable and permitted by law. The Court stated that telephonic communications are, in their nature, akin to conversations which a person he makes with an interlocutor, while enjoying the privacy of his home; thus, the privacy of these conversations is a fundamental right.

It may be noted that in interpreting Article 14, Pakistani Courts have repeatedly borrowed from the jurisprudence developed by activist Indian courts while interpreting an identical provision in the Indian constitution. In cases such as People's Union for Civil Liberties v. Union of India (AIR 1997 SC 568), Indian courts too have adopted a very broad notion of the constitutional right to privacy. These judgments are not technically part of Pakistani law; but they can be highly per-suasive when cited as precedents.

29. Jehangir Mehmood Cheema v. Federation of Pakistan (PLD 2015 Lahore 301); Muhammad Akbar Azad v. Federation of Pakistan (PLD 2015 Balochistan 69); Haji Lal Muhammad v. Federation of Pakistan (PLD 2014 Peshawar 199); Chamber of Commerce and Industry, Quetta v. Director General, Quetta Development Authority (PLD 2012 Balochistan 31); Nadeem alia Pappu v. The State (2009 P Cr. L J 744); Bashir Ahmed v. Maqsood Ahmed (2010 P Cr. L J 1824); Manzoor Ahmed v. The State (990 M L D 1488); Sardar Begum Faruqui v. Rashida Khatoon (1990 CLC 83); and Bilal Bhutto Zardari v. KDA and Other (PLD 1992 Karachi 67).

iv. Statutory Provisions on Data Privacy

At the sub-constitutional plane, there exist several statutory provisions which guarantee the pri-vacy of various kinds of data.

v. Privacy of Electronic Transaction Data and Information Systems

With respect to electronic transactions data, the basic legislation in field is Electronic Transac-tions Ordinance, 2002 (hereinafter "ETO"). The primary object of ETO was to bring legal recog-nition to electronic documents, so that they would become admissible as evidence in courts. However, once the legal significance of electronic documents had been enhanced, a need was felt for ensuring their security. Therefore, ETO also contains sections which criminalises various kinds of violations of data privacy. Section 36 and 37 of ETO are reproduced below:

Section 36. Violation of privacy of information. Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorised to gain access, as aforesaid, shall be guilty of an offence under this Ordinance punishable with imprisonment of either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both.

Section 37. Damage to information system, etc.

(1) Any person who does or attempts to do any act with intent to alter, modify, delete, remove, generate, transmit or store any information through or in any information system knowingly that he is not authorised to do any of the forego-ing, shall be guilty of an offence under this Ordinance.

(2) Any person who does or attempts to do any act with intent to impair the operation of, or pre-vent or hinder access to, any information contained in any information system, knowingly that he is not authorised to do any of the foregoing, shall be guilty of an offence under this Ordinance.

(3) The offences under sub-section (1) and (2) of this section will be punishable with either de-scription of a term not exceeding seven years or fine which may extend to one million rupees, or with both.

Both offences are related to "information systems". This term is defined quite broadly: "an elec-tronic system for creating, generating, sending, receiving, storing, reproducing, displaying, re-cording or processing information." Therefore, the scope of the offences is quite wide. Many breaches of data privacy are preceded by attempts at obtaining unauthorized access to elec-tronic data ("hacking"). ETO makes this a very serious offence.

v. Privacy of Citizens' Identity Database

One of the largest repositories of personal data in the country is the one which is maintained by the state itself: the citizenship register. In Pakistan, the National Database and Registration Au-thority (hereinafter "NADRA") which was created through Ordinance, 2000 maintains an elec-tronic register of all citizens which includes, amongst other things, the names of a citizen's par-ents and siblings, spouses and children, if any, as well as residence, date of birth and finger-prints. At the same time, the NADRA Ordinance itself places upon the NADRA the responsibility to take steps for ensuring the security and privacy of citizens' data. Relevant parts of the NADRA Ordinance are reproduced below.:

Section 5. (4) In particular and without prejudice to the generality of the foregoing powers and functions, the Authority... (d) shall ensure and provide by regulations for the due security, se-crecy and necessary safeguards for protection and confidentiality of data and information con-tained in the registration and database systems developed, established or maintained, or so caused to be developed, established or maintained, under this Ordinance including any database, data warehouse and networking infrastructure;

Section 7. National Data Warehouse. —(1) The Authority shall be responsible for... (j) ensuring of due security, secrecy and necessary safeguards for protection and confidentiality of data and information contained in or dealt with by the National Data Warehouse at individual as well as collective level.

Section 28. Information not to be divulged. Any person who—

(a) being a person employed for the purposes of this Ordinance, publishes or communicates to any person, otherwise than in the ordinary course of such employment, any information acquired by him in the course of the employment; or

(b) having possession of any information which to his knowledge has been disclosed in contra-vention of this Ordinance, publishes or communicates that information to any other person, shall be punishable with imprisonment for a term which may extend to five years, or with fine which may extend to one million rupees, or with both...

Section 29. Security, secrecy, etc. of data not to be breached. —(1) No person shall use, or deal with, or do any other thing or act of omission or commission in relation to—

(a) The registration or database systems developed, established or maintained, or so caused to be developed, established or maintained, under this Ordinance including any database, data warehouse or networking infrastructure; or

(b) The data or information contained, or housed, or transmitted therein, in contravention of the regulations made under clause (d) of sub-section (4) of section (5).

(2) Whoever contravenes the provisions of sub-section (1) shall be punished with rigorous im-prisonment for a term which may extend to fourteen years, or with fine commensurate with the nature of offence and harm, if any, caused to a particular registration or, database system as aforesaid by such contravention, but in any case not less than one million rupees, or with both.

It is worth pointing out that although the NADRA Ordinance contains these strongly-worded data privacy provisions, thus far, these provisions have been honoured only in the breach. Our re-search confirms that 17 years after the promulgation of the NADRA Ordinance, the Authority has yet to frame the data security regulations which it was obliged under Section 5 to frame. Likewise, although Section 28 and 29 stipulate harsh sentences for NADRA employees who violate data privacy and security requirement, in reality, no NADRA employee has ever been prosecuted, leave alone convicted, under these regulations.

vi. Privacy of Banking Data

The community of bankers has long recognized its obligation to ensure confidentiality of infor-mation relating to the affairs of customers. In 1997, the primary banking statute in Pakistan – Banking Companies Ordinance, 1962 – was amended in order to codify this customary re-quirement. Section 33A was inserted in order which is reproduced below:

Section 33A. Fidelity and secrecy.— (1) Subject to sub-section (4), every bank and financial in-stitution shall, except as otherwise required by law observe the practices and usage customary among bankers and, in particular, shall not divulge any information relating to the affairs of its customers except in circumstances in which it is, in accordance with law, practice and usage customary among bankers, necessary or appropriate for a bank to divulge such information.

(2) Every president, chairman, member of the Board, administrator, auditor, adviser, officer or other employee of any bank and financial institution shall, before entering upon his office, make a declaration of fidelity and secrecy in such form as may be prescribed.

The scope of this section was explained in great detail by the Lahore High Court in M. D. Tahir Advocate vs. Director, SBP M.D. Tahir Advocate vs. Director, State Bank of Pakistan and Oth-ers (2004 C L D 1680). In this case, the State Bank of Pakistan had issued a circular obliging all commercial banks in the country to share income data of their account holders with the tax au-thorities. The Court emphasized the duty of banks to ensure confidentiality of their customers' data and, relying upon Section 33A, struck the circular down.

In addition to the general duty of banks to ensure privacy of account-holders' data, there are some special provisions regarding electronic bank or online banking. These are reproduced below:

vii. Payment Systems and Electronic Fund Transfer Act, 2007

Section 70. Secrecy and Privacy.- (1) A Financial Institution or any other Authorized party shall, except as otherwise required by law, not divulge any information relating to an Electronic Fund Transfer, affairs or account of its consumer, except in circumstances in which, according to the practice and usage customary among bankers, it is necessary or appropriate for a Financial In-stitution to divulge such information, or the consumer has given consent therefor.

(2) No person other than an officer or agent appointed by the Financial Institution that maintains the account of a consumer may have access through an Electronic Terminal to information re-lating to Electronic Fund Transfer, the affairs, or the account of the consumer.
(3) The rules governing the operation of individual accounts will be applicable to Electronic Fund Transfers in relation to disclosure of information to third parties.

A Summary of the Provisions of Electronic Data Protection Bill 2005

Preamble

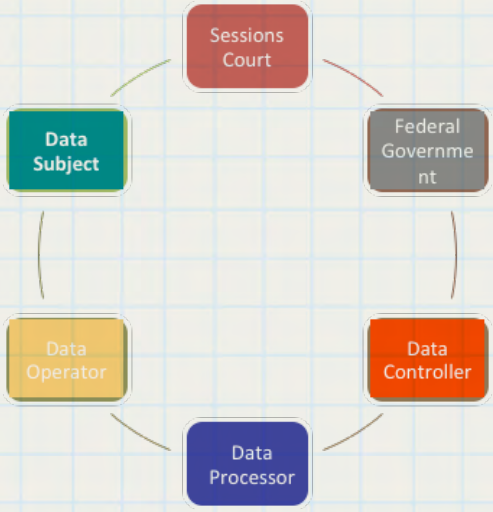
The purpose of the Electronic Data Protection Bill, 2005 (hereinafter "the Bill"), as stated in its Preamble, is ***"to provide for the processing of electronic data while respecting the rights, free-dom and dignity of natural and legal persons, with special regard to their right to privacy, secre-cy and personal identity..."***

In order to fully appreciate the duties imposed and rights protected by the Bill, we must bear in mind the following themes (i) the key stakeholders envisaged in Bill and their rights and obligation (ii) the types of data defined therein; (iii) offences against data privacy and (iv) the procedure for seeking remedies against breaches of data privacy.

Key Stakeholders

The key stakeholders envisaged in the Bill are six (6) in number:

1) Data Subject,
2) Data Controller,
3) Data Operator,
4) Data Processor,
5) The Federal Government and
6) Courts.



The definition of Data Subject is simple and unambiguous: *"the individual or person to whom the electronic data are related"*. In other words, data subject is the consumer.

There are supply-side stakeholders: Data Controller, Data Processor and Data Operation. A Data Controller is defined as "the individual or person, who determines the purposes and means of the processing of electronic data including security issues", a Data Processor is defined as "the individual or person, who processes electronic data on behalf of a data controller", and Data Operator is defined as "an individual employed by data processor for the processing of electronic data".

Perhaps a concrete example will make this clearer. In the case of an Internet Service Provider such as Nayatel, it is clear that employees of Nayatel who handle the technological aspects of the operation would qualify as Data Operators, while persons as Nayatel itself or its senior management would qualify as Data Processors. The meaning of the third stakeholder – Data Controller – is, however, not very clear. Even after a thorough reading, the meaning of this term remain unclear and this may be attributed to faulty drafting.

The Bill also vests the Federal Government with a great deal of delegated legislative authority. The Federal Government is expected to make rules governing the following areas:

1. Instructions for Data Processing (Section 5)
2. Minimal Precautionary Security Standards for custody, control and processing of Electronic Data (Section 11)
3. Conditions for Mandatory Data Disclosure (Section 14)
4. Minimal Precautionary Security Standards for custody, control and processing of Sensitive Personal Data (Section 15)
5. Conditions for Transfer of Data Abroad (Section 16)
6. Procedure for Lodging of Complaints in Sessions Court (Section 18)

Obligations and Rights of Stakeholders

The Bill creates a chain of obligations for the supply-side actors: The Data Controller must give instructions regarding how to process data. The Data Processor *"shall perform the data pro-cessing ... according to the instructions received from the data controller..."* Section 5(1)). The Data Operator, in turn, must act "only according to the instructions of the data proces-sor"(Section 5(2)). Likewise, Section 11 prescribes that electronic data must be *"processed in such a way as to minimize the risk of .... unauthorized access... or processing for purposes other than those for which the electronic data were collected"* Furthermore, the default status of all data collected or processed by Data Controller is confidential. He is prohibited from disclosing or disseminating it except where there is a contractual or statutory requirement to this effect. (Section 14).

The most significant right conferred upon Data Subject is that whenever data is being collected from him or her, he or she must given a minimum amount of information in writing.

This includes information about the purposes for which the data is being collected, whether replies to the questions are obligatory, possible consequence of his failure to reply, the recipients to whom data may be disclose and the particulars of the data controller and processors. (Section 8(1)). No data may extracted from the data subject without his consent (Section 9).

There is, however, one major exemption provides in this scheme of rights and obligations re-lated to data privacy. Section 4 gives a blanket exemption to the Government and is reproduced below:

4. Government activity and exemptions. – (1) This Act does not apply to the processing of per-sonal 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.

Electronic Data and Its Types

The Bill does not deal with privacy of all kinds of data; it deals only with Electronic Data which is defined as *"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 and includes personal, corporate, foreign and local data..."* The definition of information is the same as that provided in ETO: *"a system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or pro-cessing information"* (Section 2).

Within the category of Electronic Data, there are two grades of data which are worthy of greater protection. The first category is Personal Data which is defined as ***"any information relating to an individual, identified or identifiable, directly or indirectly..." Even more worthy of protection is the "Sensitive Data" defined as "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 provides information as to the health or sexual life of an individual and financial or proprietory confidential corporate data.*** (Section 2)

Offences and Penalties

There are numerous offences defined in the Bill, each with its own range of possible penalties. For ease of understanding, the offences and their penalties are summarized in the table below:

Section	Offence	Range of Penalties
19	Unlawful Processing of Electronic Data.	< 3 years imprisonment or < 3 million rupees fine or both
20	Unlawful Dissemination and Disclosure of Electronic Data	< 3 years imprisonment or fine (no limits described) or both
21	Unlawful Processing, Dis-semination and Disclosure of Sensitive Data	< 5 years imprisonment or fine (no limits described) or both
22	Failure to adopt appropriate data security measures	< 3 years imprisonment or fine (no limits described) or both
23	Failure to comply with orders of the Ses-sions Judge	< 3 moths imprisonment or fine (no limits described) or both
25	Corporate Liability (i.e complicity of a su-pervisor, manager etc. in above-men-tioned offences)	< 10 million rupees fine

Remedies for Breach of Data Privacy

Investigation and Adjudication Procedure

The Bill lays down a somewhat unusual procedure for a victim seeking remedies for breach of his or her data privacy. The usual procedure in dealing with special-ized crimes is to set up dedi-cated law enforcement agencies which registers complaints filed by victims, conducts investiga-tions and, where necessary, arrests and prosecute accused persons before an impartial court of law.

Instead, the Bill prescribed a variant of the procedure which is known in the Pa-kistani legal community as "the Private Complaint procedure." In the scheme of things envisaged by the Bill, any victim (or their lawyer) is expected to do his or her own preliminary investigation and put together a complaint which is to be filed in the Session Court. If a prelimi-nary case is made out in the Complaint, the Session Judge is expected appoint an investigating officer, who could just as well be a private sector professionals who commands the judge's confidence. The Investigation Officer is then vested with lawful powers of search and sei-zure and is expected to complete his work and submit a report to the Ses-sion Judge. On the basis of the report, the Session Judge may or may not con-vict the accused. A similar procedure is found in the Competition Act, 2010.

Excerpts from Section 18, the relevant provision of the Bill, are reproduced below:

18. Complaint... (2) ... [A]ny data subject ... may lodge a complaint against any data controller ... to the Sessions Judge, having territorial jurisdiction, for enforcement of his rights or interest under this Act or any ... contract.

(3) The Sessions Judge, if feels necessary, may direct any person or individual to inves-tigate into the complaint lodge before him and report back to the court..

(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) ... [T]he 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 elec-tronic data, the rights and interest of the complainant and ensure compliance of the applicable provisions of this Act, rules and the contract...

(8) Any final order of the Sessions Judge may be appealed against by any aggrieved in-dividual or person as First Appeal against Order before the High Court having territorial jurisdiction, within thirty days from the communication of the said order.

As supervisor of investigations, the Sessions Judge have been vested with the all-important power to issue "Stay Orders". This is stated in sub-section (6) of Section 18.

(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 oper-ations of processing.

The Sessions Judge is also entitled to all the support he can get from the law enforcement au-thorities, ie. the Police Department and Federal Investigation Authority etc. This is stated in sub-section (7) of Section 18.

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

ix. A Critique of the electronic data protection bill, 2005

Overall, the drafting of the Electronic Data Protection Bill is a welcome step which should be hailed as a step in the right direction. As pointed out earlier in this report, although Pakistan does have statutory provision providing for data privacy in certain segments of life, a generalized data privacy law remains to be adopted. It is therefore unfortunate that more than 12 year after a Bill for this purpose was first drafted and introduced in Parliament, no further legislative progress has been made.

While represents a welcome start, in its present form the Bill suffers from serious shortcomings. It must be debated widely and critiqued professionally before being adopted. Some views on it are offered below.

Lack of Clarity: Data Controller and Data Processor

Firstly, the entire scheme of the Bill is confusing. More than anything else, a good law is a law which can be understood by all and sundry, without having to consult a lawyer. The Election Da-ta Protection Bill is far from that, an error which may be attributed more than anything else to careless and unskilled drafting.

The distinction between data controller and data processor is, for instance, hard to grasp even for trained legal experts. It is possible that this distinction was drawn in view of some technolog-ical realities which in 2017 no longer exist.

If so, we are of the view it would be better to simply do away with this distinction. Instead, the only practical distinction which needs to be drawn should be between those who collect data, those who process it and those who transmit it. All three should be included in the law's ambit. However, the data privacy rules to be framed for all three should be different.

Lack of proportionality in regulatory requirements and punishments

Furthermore, the Bill draws no distinction between the compliance obligations incurred by commercial entities of various sizes. The onus of compliance placed upon a data processor who processes 1 GB of data appears to be the same as that upon a data processor who processes 1million GB. This violates the universal legal principle of proportionality.

In our opinion, it would be better to altogether exclude from the regulatory ambit all data collec-tors, processors and transmitters who deal with a relatively small volume of data – say 100 r 1,000 GB of data. Likewise, the onus of compliance upon those entitled which do fall within the regulatory ambit should to be proportionate to the volume of data handled by them. So, for in-stance, the diligence and investment required for a small data processor should be less and that required of a bigger company should be more.

A similar lack of proportionality can be seen in the offences envisaged in the Bill. The punish-ments awarded for offences stated in Section 19 and 20 etc. should be proportionate to the commercial size of the violator and the extent of harm suffered by the victim. At present, this issue has been left to judicial discretion. We are of the view that it should be explicitly stated in the section relating to offences.

The Blanket Exemption granted to the Government

The Blanket Exemption granted to the Federal Government in Section 4 of the Bill is completed unacceptable and goes against the principle of equality before law enshrined in Article 25 of the Constitution. To the extent that the Federal Government engages in the business of data pro-cessing, it should be expected to abide by the same standards of data privacy as everyone else. Of course, insofar as the requirement of criminal law or regulatory are concerned, the Federal Government would be able to waive off privacy rights of customers just like all other data pro-cessors. However, to place it completely beyond the pale of law is tantamount to opening the door or authoritarianism which runs against the principles of Pakistani Constitution.

Unique Investigation and Adjudication Mechanism

It is questionable whether the unique investigation and adjudication mechanism method envis-aged in the bill – a variant of the private complaints method – would be workable. While Sessions Judges are likely to be more independent than career investigators, it remains to be seen whether they would be able to spare the time or have the technical intellectual capacity required to deal with issues of data privacy.

It would perhaps be better to set up an independent, tenured, statutory commission on Data Privacy and task with registering and investigating complaints and, if necessary, prosecuting. Insofar as adjudication is concerned, it would be best to set up a specialized Data Privacy Tri-bunal for dealing with relevant offences. A dedicated Commission and dedicated Tribunal staffed by senior professionals drawn from the field of IT and Law would better be able to muster the time and resources which this issue requires.

x. Overall need for comparative analysis

We believe that Pakistan does not need to reinvent the Bill and any legislative exercise in the field of data privacy should be preceded by a through comparative law review. The issue of Data Privacy is not unique to Pakistan. It is a global issue. Over the last couple of decades, statutes for dealing with Data Privacy have been drafted and promulgated the world over, an excellent summary of which has been prepared by the law firm DLA Piper.[32]

32. DLA Piper. https://www.dlapiperdataprotection.com/

Our preliminary review of existing data privacy legislation from across the world indicates that perhaps the most suitable model for Pakistan is the model law prepared by Center for Internet and Society, India. This model law which is titled The Privacy (Protection) Bill, 2013 enjoys three advantages over Pakistan's Electronic Data Protection Bill, 2005: one, it has a more logical flow and is easier to comprehend; two, it is more comprehensive; and three, it is more in line with the technological realities of 2017. Therefore, when the Pakistani Parliament turns its attention to this matter, it would be useful to thoroughly review the Privacy (Protection) Bill, 2013 drafted by CIS and to borrow from it extensively.

Comparative Global Analysis of Data Protection Legislation

To provide for comparative analysis of global legislation on data protection, this study looks at:

vii. Regulation on Protection of Natural Persons with Regard to Processing of Personal Data and on Free Movement of such Data / General Data Protection Regulations, GDPR (2016), European Union (EU)[33]

i. Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (as revised in 2013), Organisation for Economic Cooperation and De-velopment (OECD)[34] [35]

ii. Convention (108) for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), Council of Europe (CoE)[36]

33. *Regulation (EU) 2016/679 of the European Parliament and of the Council. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*
34. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm*
35. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf*
36. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/1680078b37*

I. Regulation on Protection of Natural Persons with Regard to Pro-cessing of Personal Data and on Free Movement of such Data / General Data Protection Regulations, GDPR (2016), European Union (EU)

Formal implementation of GDPR which was adopted in 2016, is scheduled for May 2018 to allow organizations a compliance preparation period of two years. The Regulations mandate that organizations including those not physically located inside the European Union (EU) but handling personal data of EU citizens will be fined "up to 4% of (their) annual revenue or up to €20 million, whichever is higher" for violations.[37]

Among GDPR's key components are Article 25 - data protection by design and by de-fault - which calls for "appropriate technical and organisational measures" such that data acquisition complies with principles of need specification and data storage complies with access and retention limitation. Privacy by design as contained in GDPR thus aims at protecting user identifiers, also including Internet Protocol credentials, through provisions like "Pseudonymisation and Encryption of personal data" (Article 32). It is noteworthy for Pakistan's context of one of the world's largest citizen biometric databases,[38] that barring exceptions of individual's explicit consent and processing required for legal necessities, GDPR through Article 9 'prohibits' processing of unique identifiers including individual's 'biometric' data.[39]

While personal data must have been acquired by expression of a 'demonstrable' con-sent by data subject, organizations must ensure that data subjects have similar ease for consent withdrawal 'at any time' (Article 7).[40] An extension of this right to consent withdrawal is the data subject's 'Right to Erasure (Right to be Forgotten)' enshrined in Article 17. This provision places responsibility with the concerned data controller to have sufficient technical capacity to ensure that all replications and copies of this data, including those made accessible by them to other data controllers, are erased without delay.[41]

37. *General Data Protection Regulation.https://www.rapid7.com/de/fundamentals/gdpr/*
38. *Pakistan's experience with identity management. http://www.bbc.com/news/world-asia-18101385*
39. *Regulation (EU) 2016/679 of the European Parliament and of the Council. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*
40. *GDPR Conditions for consent. https://gdpr-info.eu/art-7-gdpr/*
41. *Ibid.*

GDPR is innovative in that it also enshrines the "right to data portability" allowing data subjects safe transfers of their data between service providers. A European Commis-sion press release from May 2017 defines GDPR's "one-stop-shop" mechanism as a way of streamlining legal uniformity across all EU member states so that "businesses will profit from faster decisions, from one single interlocutor (eliminating multiple contact points)." According to this press release, the right to data portability combined with the one-stop-shop mechanism will make data markets fairer and competition-friendly for smaller EU companies which otherwise struggle against data giants, especially by cutting compliance costs. This can be understood in the context that currently, under the various EU data regulation regimes, individual franchise outlets of a company which for example is headquartered in a different EU country, all have to individually comply with the specific national data regulation of the EU state of their location. This means that the company has to ensure separate compliance for each of its national franchises thus amounting to quadrupled costs.[42] Innovativeness of GDPR is also in its formalization, under Section 3, of the requirement from data controllers to conduct Data Protection Impact Assessments (DPIAs) particularly for high-risk data processing, to determine proportionate safety measures.[43]

Under GDPR, data-handling organizations are required to formalize a watertight 'Data Breach Notification' process to mandatorily report every data breach to the EU member state GDPR Supervisory Authority within 72 hours of the incident. The breach 'may' also need to be reported to those affected, depending upon its scale and nature.[44] However, to provide for a more proactive than reactive approach to data protection, GDPR, along its length, stresses on periodic system audits interpreted as audits of 'not just technology, but people and processes, too.'[45] Also notable is the constitution under GDPR of the European Data Protection Board (EDPB). The Board will have representation of the cross-EU national data protection authorities, of the European Data Protection Supervisor, and of the European Commission. EDPB's role is not only advisory; decisions of the Board, on certain disputes between national data protection authorities, will be binding.[46]

42. *European Commission - Fact Sheet. http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm*
43. *Regulation (EU) 2016/679 of the European Parliament and of the Council. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*
44. *General Data Protection Regulation. https://www.rapid7.com/de/fundamentals/gdpr/*
45. *Ibid.*
46. *European Commission - Fact Sheet. http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm*

Data controllers and processors are required under Article 37 to designate a 'data protection officer (DPO)'. The size of the organization requiring the appointment of a DPO is however not clarified. Prevalent inference is that while well-resourced organizations are to create a designation for a full-time DPO, smaller organizations may do with a part-time or even virtual position for a DPO. But again, GDPR contains no clear direction on what defines a 'well-resourced' or a 'smaller' organization. Furthermore, EU's burgeoning "Big Data" industry with 23 million small and medium sized enterprises (SMEs) will be a challenge to consistent implementation of some of GDPR's ambitious propositions like the appointment of Data Protection Officers (DPOs) and the "unreasonable" data breach notification deadline of 72 hours.[47] These challenges can also be viewed in Pakistan's context of ill-equipped, under-resourced SMEs, some with serious financial and human resource constraints to question their readiness to regulate data processing, let alone ensure data protection, in the face of evolving ICTs "and practices, such as Big Data, BYOD (Bring Your Own Device), cloud computing, geolocation services, cookies and social networks."[48] Another critique of the Regulations is its recurrent use of vague terminologies; for in-stance, 'appropriate' and 'state-of-the-art' with no unambiguous, supplementing directions on the definitions of these terms.[49] It can thus be argued that because GDPR's language itself does not contain extensive, detailed supplementary guidelines regarding the mechanism to practically operationalize the Regulations, it may not yet be described "as a ground-breaking instrument" before its implementation comes through.[50]

Article 5 makes processing of personal data operational under GDPR, through six principles. Principle (a) mandates that personal data is processed "lawfully, fairly, and in a transparent manner."[51] This is interpreted as requiring demonstrable consent from data subjects before data is collected or processed, and as recommending mechanisms which allow data subjects to practice explicit refusal and/or negation of consent via "opt-out." These six principles in essence are similar to the Privacy Principles contained in the

47. *The Data Protection Regulation: A Triumph of Pragmatism over Principle? http://edpl.lexxion.eu/data/article/10075/pdf/edpl_2016_03-006.pdf*
48. *What does the revision of the OECD Privacy Guidelines mean for businesses? https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf*
49. *Making Sense of the General Data Protection Regulation. https://www.tripwire.com/state-of-security/security-data-protection/making-sense-general-data-protection-regulation-gdpr/*
50. *The Data Protection Regulation: A Triumph of Pragmatism over Principle? http://edpl.lexxion.eu/data/article/10075/pdf/edpl_2016_03-006.pdf*
51. *Regulation (EU) 2016/679 of the European Parliament and of the Council. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*

New Zealand Privacy Act of 2013. For instance, Principles (b), (c), (d), (e), and (f) respectively provide that data collected is 'absolutely' relevant to purpose specified, that this data is updated and accurate to avoid any probable harm to data subject, that its retention is stringently limited and follows complete erasure, and that systems and protocols are security-appropriate to maintain data confidentiality. It is debatable and will be determined by how organizations eventually upgrade their capacities in compliance with GDPR, whether or not the Regulations rely more heavily on organizational measures and thus discount the "need for technological solutions."[52]

Explanation of 'lawful (personal data) processing' given on the website of UK's Information Commissioner's Office, includes that lawful basis for this processing should be well-documented. Under Article 6, the Regulations list out - that consent given by data subject for such a processing; that this processing being necessary (though it remains vague on the parameters against which this 'necessity' is to be determined) for "performance of a contract with the data subject"; that such a processing being necessary to ensure public interest or other legal compliances and to ensure data subject's interests - constitute this 'lawful' basis.[53]

II. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (as revised in 2013), Organisation for Economic Cooperation and Development (OECD)

Not legally-binding and thus carrying minimal legal weightage, the OECD Guidelines, published in 1980 and most recently revised in July 2013, were among the very first internationally agreed-upon regulations on data protections.[54] Data protection framework of the Guidelines is carried through 8 privacy principles which are listed under Part Two – Basic Principles of "National" Application as distinct from Part Three – Basic Principles of "International" Application, of the Guidelines.

Among these 8 principles, while the 'Collection Limitation Principle' mandates a "lawful and fair" collection of data, it makes conditional the bringing into knowledge and the taking of consent of the data subject vis-à-vis collection of their data, upon "where appropriate", thus largely empowering the subjective discretion of the data collector in this matter. The 'Data Quality Principle' provides that data collected must be up to date, accurate, and proportionate to the limited and specific purposes of its acquisition which

52. *The Six Commandments of the GDPR. https://www.tripwire.com/state-of-security/security-data-protection/six-commandments-gdpr/*
53. *Information Commissioner's Office. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/*

"should be specified not later than at the time of data collection" thus substantiating the 'Purpose Specification Principle' and the 'Use Limitation Principle' which also discourages such a disclosure of this data which was not specified during its collection (except for when "authority of law" and data subject's consent allow)). The 'Security Safeguards Principle' provides that "reasonable" security mechanisms should be emplaced to ensure the collected personal data's security. Notable are the 'Openness', the 'Individual Participation', and the 'Accountability' principles. Respectively, these 3 principles provide for, a "general policy of" transparency to be guaranteed through such mechanisms which allow easy access to information regarding personal data; individual's right to have communicated to them within reasonable time and as applicable, against reasonable fee, information about their personal data being collected and / or held, along with the intimation to them about their right to challenge and subsequently get erased or amended any such personal data being held; the accountability of the 'data controller' to comply with the principles.[55]

These privacy principles set out benchmarks for future guidelines on data protection, as is sufficiently reflected through the language around privacy principles in both, the New Zealand Privacy Act[56], and, GDPR. As with GDPR, one of the perspectives regarding the revised OECD Guidelines is also that they focus on "organisational responsibility", as translated through organizational reforms related to processes and personnel, rather than on tangible technological solutions, by for in-stance placing "more emphasis on the controllers' responsibility", here through the 'Accountability Principle' and the newly added section 'Privacy Management Programmes' wherein data controllers now have an added obligation to establish demonstrable privacy safeguards - like employee preparedness, internal and external audits, and greater compliance written into contractual provisions - around "privacy risk assessment, an internal governance structure, oversight mechanisms, and incident response plans".

54. *What does the revision of the OECD Privacy Guidelines mean for businesses? https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf*
55. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm*
56. *Privacy Act, 1993 (New Zealand) http://www.legislation.govt.nz/act/public/1993/0028/latest/whole.html#DLM296639*

The coverage of these Programmes will now not only address the operations of the data controller but also of the operations of their employees and agents.[57] [58]

'Data security breach notification', a renewed emphasis on designing policy frameworks on 'education and awareness', on development of skills of privacy professionals as part of 'National privacy strategies', and on improving "global interoperability of privacy frameworks through international arrangements" are among the few increasingly focused provisions of the revised Guidelines.[59] The Report on the Review of the 1980 OECD Privacy Guidelines, prepared by the Privacy Expert Groups of the OECD Working Party on Information Security and Privacy (WPISP), and which played a critical role in informing the revision of the 1980 Guidelines, mentions data subject's 'consent', the 'purpose specification', 'use limitation', 'openness', and 'individual participation' principles, definitions of 'personal data' and 'data controller', role of "other actors" like individuals and organizations which 'design' systems through which data collection and processing occur, as areas of the Guidelines on which revisions were proposed.[60]

Trans-border data flows, revised through a more stringent 'risk-based approach' feature prominently in the 2013 Guidelines. The revised approach discourages the previous 'one size fits all' approach, calling for businesses to bring into policy and practice privacy management programmes which are adaptable to specific business needs.[61]

57. *What does the revision of the OECD Privacy Guidelines mean for businesses? https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf*
58. *The OECD Privacy Framework. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*
59. *Ibid.*
60. *Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines. http://www.oecd-ilibrary.org/docserver/download/5k3xz5zmj2mx-en.pdf?expires=1499213942&id=id&accname=guest&checksum=52E2238F04124B76767B3250C3C38636*
61. *What does the revision of the OECD Privacy Guidelines mean for businesses? https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf*

III. Convention (108) for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), Council of Europe (CoE)

Opened for signatures in January 1981, Convention 108 "is still today the only binding international treaty in this field. It is open (for signatures) to any country, and has the potential to become a global standard. 46 member states of the Council of Europe and Uruguay are state parties, whereas Mauritius, Morocco, Senegal, and Tunisia have been invited to accede."[62] Since 2016, a final proposal for the Convention's revision is being prepared which is aimed at ensuring its consistency with EU's GDPR.[63] This modernization of the Convention calls for more extensive and elaborate yet technologically-neutral cross-sectoral legislation to be introduced by signatories at their respective national levels. This modernization process also innovates the Convention by placing emphasis on pursuing the 'proportionality and minimisation' of data's collection, on signifying the roles of data controllers and processors with regards to ensuring accountability and data-processing transparency, on guaranteeing 'privacy by design', and on declaring data breaches through obligatory notification mechanisms. Notably, transmission of data from a Convention signatory to a non-signatory requires that it is ensured before this transmission that the recipient territory has "appropriate level of protection" for data's secure handling, processing, and storage however still somewhat conflicting is the Convention's Article 12 according to which a Party shall not stop or require 'special authorisation' of any data being transmitted to the territory of another Party.[64] [65]

Among provisions regarding 'Quality of data' collected, similar to those contained in the other aforementioned legislations, Article 5 of the Convention is notable in that it requires that data collected should be preserved in such a manner that it does not allow for the 'identification' of data subject after the time period of the data's retention has passed.

62. *Modernisation of the Data Protection. http://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet*
63. *Regulation (EU) 2016/679 of the European Parliament and of the Council. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*
64. *Modernisation of the Data Protection. http://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet*
65. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37*

Article 6 specifies data which carries potential to reveal "racial origin, political opinions or religious or other beliefs" along with personal data regarding health and sexual life and regarding criminal convictions, as a 'Special' category of data, the processing of which shall only occur when legislation, procedural regulations, and directives of the domestic law guarantee sufficient processing safeguards. Building upon the same, Article 8 provides for 'Additional safeguards for the data subject' – including being able to obtain "without excessive delay or expense" information about the existence of a data file containing personal data about them, besides being able to acquire further details about the purpose of its collection, storage, and processing, and, besides being able to obtain its rectification and erasure. However, the Convention also affords arbitrary exceptions to the application of these safeguards. Contained in Article 9 of the Convention, one of these exceptions is 'protecting State security', which in the absence of very specific accompanying guidelines and case studies, can be used to draw vague interpretations to infringe potentially wide-ranging limitations on these safeguards. Article 11 calls on the signatory Parties to not treat the Convention as a limiting or complete framework and to explore the possibility of building upon the Convention to provide "wider" protections to their data subjects (through supplementary domestic laws). These protections also include that any authority which as a consequence of its designated mandate, receives any information from another authority, should not use out of its own accord, this information for a purpose other than that for which it requested the information from the other authority; this has to be ensured by binding authority personnel by "appropriate obligations of secrecy or confidentiality with regard to that information."[66] It is felt that text under Article 16 (of the Convention) when read as a standalone re-quires further guidelines on how the possibility of conflict among authorities (of different signatory States) can be prevented and inter-State harmonization ensured through a case-by-case review, when the designated authority of one Party can, under this Article, refuse to comply with a request made by the designated authority of another Party for information assistance.

It is also felt that the Convention should contain explanatory text marking clearer distinction in definitions of States (Contracting States), Parties, and Authorities. However, according to the simultaneously published 'Explanatory Report to the Convention (1981),' the grounds on which an authority can refuse to comply with an information request are restricted and are the grounds which generally occur in international mutual assistance treaties.[67]

66. Ibid.
67. Explanatory Report to the Protection of Individuals with Regard to Automatic Processing of Personal Data. https://rm.coe.int/16800ca434

Besides, the Convention's provision on the role of the 'Consultative Committee' de-serves attention. It is defined in Chapter V of the Convention, as a committee constitut-ed to formulate proposals, opinions, and amendments (which may also be proposed by a Party, or, Council of Europe's Committee of Ministers, to the Consultative Committee for its opinion, for eventual approval by the Committee of Ministers) to facilitate the Convention's understanding, improvement, and application.[68]

According to the Explanatory Report, despite the presence of previously established legal rules around the handling of sensitive private information, guidelines to determine an individual's control over their own information were lacking. Convention 108 – which was also informed by input from the Organisation for Economic Cooperation and Development's (OECD) own evolving policy guidelines in the field of ICTs – despite its non self-executing character, provided for a holistic direction regarding this. National legislations by the Convention's signatory States still had the liberty to continue to differ on defining procedural features; for example, the national data privacy legislation of some States regulated data processing by the public sector only, while others also regulated data processing by the private sector. Similarly, while coverage of this national legislation in some States, included only automated data, national legislation of other States also included categories of manual / manually-processed data. While legislation in all countries applied to 'data relating to natural persons,' in some it also applied to data 'concerning legal persons.' The explanatory document acknowledges that the Convention was needed to respond to the challenges which existed for free trans-border data flow – in that, while attempts by data users and organizations to transfer their operations to 'data havens' which had lenient data protection regulation had to be discouraged and curbed through regulation, it had to be simultaneously ensured that smooth flow of data across borders is not hindered owing to stricter regulation. Similarly, the Explanatory Report acknowledges that the respective national legislation by States should be allowed to vary – for instance, the 'legitimate purpose' for the storage and collection of data is specified according to these State-specific national legislations and may not be in uniformity with those of other State parties.[69]

68. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37*
69. *Explanatory Report to the Protection of Individuals with Regard to Automatic Processing of Personal Data. https://rm.coe.int/16800ca434*

It should be noted that the Explanatory Report makes specific mention that "personal data concerning health" which is categorized as a Special category of data under Article 6 of the Convention, has been defined as data "concerning the past, present, and future, physical or mental health" of a "sick, healthy, or deceased" individual, also covering data related to intake of drugs or alcohol by them, by the 'Committee of Experts on Data Protection' based on their study of medical data banks. Regarding the security of data collected and stored (Article 7 of the Convention), the Report prescribes that security measures are to be specific for every file depending upon its specific level of vulnerability.[70]

The Report underscores that for every personal data collected, the controller of its data file - defined as the "person or body ultimately responsible for the file, not persons who carry out operations according to instructions given by the controller" - should be clearly identified either through a list published in a public index or directly communicated to data subject on their request. Explanation provided in the Report, for Convention's Article 9 - 'Exceptions and restrictions' merits careful observation. It provides that any exceptions afforded to provisions of the Convention are not to exceed those needed for the safeguard of "fundamental values in a democratic society" in conjunction with safeguard of what is traditionally acknowledged as "State security" including also the protection of State's international relations, and that of everything which finances the State's policies and its "monetary interests". Informed by decisions of the European Commission and of the European Court of Human Rights, and modelled after the European Human Rights Convention, Convention 108 acknowledges that these exceptions cannot be defined for all signatory States and for all times to come, and will have to be defined specific to a present scenario for each State. On the Convention's Chapter III, Trans-border data flows, the Explanatory Report carries exhaustive elaboration. It records that trans-border flow of any data is to be determined with reference to the data's "mode of representation", for example 'plain or encoded text'; where the data is stored, for example on 'paper, magnetic tape, or disk'; medium on which the data is transported, for example via 'mail or telecommunications link'; the data's transfer route, that is, the origin-transit-destination besides other considerations. This also implies that the collection of data is also to be subject to these provisions on the trans-border flow of data, that is, the provisions apply also to "data gathered in one country and processed in another." Data imports are not affected under these provisions and are to be primarily regulated under data protection frameworks of the State which is importing the data.[71]

70. Ibid.
71. Ibid.

An Additional Protocol to the Convention, signed in November 2001, provided for a 'completely independent' function of Supervisory Authorities. According to this Protocol, each Party shall designate such supervisory authorities vested with the "powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law." The broader role of these authorities, the Protocol mentions, will be to ensure compliance with initiatives taken to further the domestic implementation of the Convention.[72]

Conclusion and Key Recommendations

As technology moves forward at a pace never seen before, the Pakistani government's attitude to privacy and protection of data remains stagnant. As of now, there is no data protection legislation in place in Pakistan. This is surprising, given the increased amount of citizens' data being processed each and every day. Pakistan is now in urgent need of data protection legislation that is not only intelligible, but also fit for purpose.

As the EU's GDPR comes into force across all EEA states next year, it is even more crucial for Pakistan to act now on data protection as benefits of introducing such legislation can be immense. Being in tune with data protection and privacy laws of other states, cannot only be beneficial economically, but also morally. Countries that respect human rights, and adhere to the rule of law will be seen as progressive and as such favouring innovation and development. This in turn, will open Pakistan to the outside world.

Failure to implement adequate data protection laws now, could soon mean that large foreign companies may begin to view Pakistan as increasingly unsafe business-wise and shun it when it comes to outsourcing their business services. Citizens on the other hand will lack confidence in their own government being able to protect their most fundamental human right that the right to privacy is. In this day and age, citizens' personal data should never serve as a tool to be used against them, and it must be protected at all costs.

Below are key recommendations that we propose based on the above report:

72. *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626*

- Amendment to PTA is necessary. The Act is incompatible with Article 17 of the ICCPR, to which Pakistan is a signatory state.
- Urgent need for an independent authority overseeing data protection compliance to be set up. Its role would be to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, as well as dealing with complaints (body similar to the British Information Commissioner's Office).
- Establishing a system of accountability for data breaches applicable to big data repositories.
- The Electronic Data Protection Bill, 2005 is not fit for purpose. Pakistan should look into adoption of data protection legislation similar to the GDPR, or alternatively draft law based on India's Privacy (Protection) Bill, 2013.
- Education of citizens about personal data and its value is urgently needed
- Including the principle of individual's consent for processing data in any new legislation is crucial and should be expressed in an unambiguous and intelligible manner. The requirement of consent, and consent withdrawal, should be part of any data collection process.
- The use of data anonymisation (pseudonymisation) mechanisms should be strongly encouraged as it reduces the risk of individual being identified by their data. The principle of data anonymisation should also be part of any new draft data protection legislation.


www.bytesforall.pk

APC
IMPACT
SEA - MALAYSIA - PAKISTAN
ADVOCACY FOR CHANGE THROUGH TECHNOLOGY

PRIVACY
INTERNATIONAL