Proposed Amendments to the Draft Personal Data Protection Bill, 2020

Submitted by:

Bytes for All, Pakistan

www.bytesforall.pk

May 14, 2020

Proposed amendments to the Draft Data Protection Bill 2020

Bytes for All, Pakistan[1]

Preliminary

The first and foremost question that may be addressed is of which item in the Federal Legislative list in the Constitution does it fall under[2]. In other words, does the Parliament have adequate legislative competence to enact this bill. It is likely to be challenged on these grounds. However, we see that the parliament may claim legislative competence under the following items of the Fourth Schedule of the Constitution:

> *1. The defence of the Federation or any part thereof in peace or war; the military, naval and air forces of the Federation and any other armed forces raised or maintained by the Federation; any armed forces which are not forces of the Federation but are attached to or operating with any of the Armed Forces of the Federation including civil armed forces; Federal Intelligence Bureau; preventive detention for reasons of State connected with defence, external affairs, or the security of Pakistan or any part thereof; person subjected to such detention; industries declared by Federal law to be necessary for the purpose of defence or for the prosecution of war.*
>
> *3. External affairs; the implementing of treaties and agreements, including educational and cultural pacts and agreements, with other*

[1] The legal analysis is prepared by Yasser Latif Hamdani o*f the Honourable Society of Lincoln's Inn - Advocate High Court in consultation with Haroon Baloch, Program Manager, Bytes for All, Pakistan. Shahzad Ahmad, the Country Director reviewed the submission.*

[2] In Pakistan is a federal parliamentary state and as such the residuary powers lie with the provinces. Therefore, the legislative competence of the parliament is limited to the Federal Legislative List given under the Fourth Schedule of the Constitution.

countries; extradition, including the surrender of criminals and accused persons to Governments outside Pakistan.

4. Nationality, citizenship and naturalization.

7. Posts and telegraphs, including telephones, wireless, broadcasting and other like forms of communications; Post Office Saving Bank.

17.Education as respects Pakistani students in foreign countries and foreign students in Pakistan.

28. State Bank of Pakistan; banking, that is to say, the conduct of banking business by corporations other than corporations owned or controlled by a Province and carrying on business only within that Province.

32. International treaties, conventions and agreements and International arbitration.[3]

Therefore items 1, 3, 4, 7, 17, 28 and 32 would clothe the Parliament with the requisite legislative competence to make the data protection law. The counter argument from those who favour provincial competence may come on grounds that there is no direct entry for data protection. This will be an issue that the government must be ready to satisfy various vested interests.

The bill in its current form is fraught with difficulties not just because of bad drafting (the sections and subsections along with cross references are not formatted at all) but also what appears to be an intentional attempt to hedge the law in exceptions and language, which will leave the door open for misuse of personal data for the purposes

[3] Fourth Schedule of the Constitution of the Islamic Republic of Pakistan 1973.

of surveillance. To avoid any confusion when this statute comes under judicial scrutiny, we strongly recommend formatting and proper capitalization of terms.

The intention of the draft seems to be giving excessive powers to the powers that be to control citizens' data. While one recognizes that any government has legitimate reasons for data processing, it should not be allowed to become a tool for phishing and unlawful monitoring of individual citizens. The right to dignity and privacy of home are inviolable under Article 14 of the Constitution of Pakistan. This fundamental right has to be safeguarded by the state as the custodian of fundamental rights of citizens. An exercise in data protection cannot be allowed to be converted into a Panopticon of surveillance. In the following section-by-section analysis an attempt has been made to bring the law into conformity with four frameworks:

1. Constitution of Pakistan;
2. International best practices;
3. Case law; and
4. Practical experience of statutes and their misuse.

This draft treats personal data of the citizens as the property of the state, with little control for the citizens *vis a vis* their data saved on public and private servers. The bill also vests the Federal Government and the proposed Authority with a lot of discretion to determine and exclude items from personal data, critical personal data and sensitive personal data.

Pakistan's experience with authorities constituted under special laws has been problematic. Authorities without exception tend to become bureaucratic and are in the final analysis always subject to the whims of the government. At the outset one must state that there should be a Privacy and Data Protection Commission instead of an Authority. Such a Privacy and Data Protection Commission should not have any ex-officio members from the ministries but should be entirely independent and vested with the powers of the civil court and under the superintendence of the relevant High

Court. Such a commission should have an internal separation of the executive and the judicial officers.

With this preliminary observation, the following are the amendments that are proposed to the bill. The original section appears italicized and the proposed amended section appears both italicized and underlined. A brief explanation is given against every amendment. Where we propose that a certain section should be omitted altogether, we have only given an explanation.

AMENDMENTS

Section 1

1.3

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

We are perturbed by the use of the term "promulgation" instead of "enactment" here. The term promulgation here presumably means the assent of the president and it is true that promulgation is used in the sense of an act receiving the assent of the president. On the other hand, the fear that arises from this is the idea that a law of such significance may be promulgated as an ordinance instead of an act. Pakistan is a parliamentary democracy and such a law should be made after reasoned debate by people's representatives and not at the whim of the executive. Nor do we understand why the time period of enforcement is kept uncertain.

We propose that this section should be reworded as under:

1.3 It shall come into force after six (6) months from the date of its enactment and for avoidance this section shall be a self-executing provision.

Section 2.

There is no comprehensive data definition. Definition of data as a whole is required to complete the definition section. That said here are our recommendations for the remainder:

2(a)

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

This should be re-worded to include both natural and legal persons, because a data subject can be a company, trust or association. Our proposed section is as under:

a) "data subject" means a natural or legal person who is the subject of the personal data;

2(g)

2 g(v) should be omitted as it is the same as data processor

2(k)

2 (k) "sensitive personal data" means and includes data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, and, passports, biometric data, and physical, psychological, and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, or any other information for the purposes of this Act and rules made thereunder.

We propose that this section should have the "video graphic data", "political affiliation", and "any other distinguishing characteristics" after "religious beliefs". Our proposed section is as under:

2 (k) "sensitive personal data" means and includes but is not limited to name, data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, and, passports, biometric data, physical, psychological and mental health conditions, all other medical records, and any detail or information pertaining to an individual's ethnicity, religious (including sectarian) beliefs, opinions, political affiliation, any other distinguishing characteristics of such individual or any other information for the purposes of this Act and rules made thereunder.

2(o)

In 2(o) the reference to "Critical Personal Data" is unclear nor is Critical Personal Data defined or distinguished from "Sensitive Personal Data"- nor can it be left to the authority to define it. We propose dropping the term "critical personal data" and using sensitive personal data instead.

Section 4

4 PROTECTION OF PERSONAL DATA

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

We propose to add the following words "and all Data Controllers, Data Processors, concerned Third Parties and Government Officials shall be under Strict Civil and Criminal Liability for failing to comply hereunder." This is self-explanatory and is because we want to build in both damages and criminal action against any departure from these provisions. We want to make is strict because we do not want *actus reus* to be subject to *mens rea*. We also believe that any departure from the provisions of this law should not be subject to intent but a duty of care on part of the Data Controller and Data Processor. Our proposed section is hereunder:

4 PROTECTION OF PERSONAL DATA

The collection, processing and disclosure of personal data shall only be done in compliance with the provisions of this Act and all Data Controllers, Data Processors, concerned Third Parties and Government Officials shall be under Strict Civil and Criminal Liability for failing to comply hereunder.

Section 5

5.2

5.2 Notwithstanding sub-section (1) , a data controller may process personal data about a data subject if the processing is necessary—

a) for the performance of a contract to which the data subject is a party;

b) for taking steps at the request of the data subject with a view to entering into a contract;

c) for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;

d) in order to protect the vital interests of the data subject;

e) for the administration of justice pursuant to an order of the court of competent jurisdiction;

f) for legitimate interests pursued by the data controller; or

g) for the exercise of any functions conferred on any person by or under any law.

We propose that 5.2 (a) should be omitted. The compliance with a contractual obligation under sub-section (a) is unclear and it stands to reason that a party to a contract will provide reasonable information of his or her own accord. Moreover, sub-sections (d) and (f) should be clearly and narrowly defined, especially the terms "legitimate interests" and "vital interests" have not been defined in Section 2, hence provide for the data controller and the processor to decide for their definitions/interpretations. These serve to dilute the safeguards and provide out-clauses to Data Controller and Data Processor. Our proposed section is as under:

5.2 Notwithstanding sub-section (1) , a data controller may process personal data about a data subject if the processing is necessary—

a) for taking steps at the request of the data subject with a view to entering into a contract;
b) for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;
c) in order to protect the vital interests (need definition) of the data subject; and
d) for legitimate interests (need definition) pursued by the data controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, or
e) for the administration of justice pursuant to an order of the court of competent jurisdiction.

5.3

5.3 Personal data shall not be processed unless—

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

We propose that in "c" the word "reasonable" should be added after "adequate" in order to make it subject to Wednesbury test[4]. The following statement should be added "The concerned Data Processor and Data Controller shall solemnly affirm

[4] A standard of unreasonableness used in assessing an application for judicial review of a public authority's decision. A reasoning or decision is Wednesbury unreasonable (or irrational) if it is so unreasonable that no reasonable person acting reasonably could have made it (Associated Provincial Picture Houses Ltd v Wednesbury Corporation (1948) 1 KB 223)

through a simple affidavit that they have only processed adequate Personal Data in accordance with this Act, a record of which shall be kept for inspection and legal purposes."

5.3 Personal data shall not be processed unless—

a) the personal data is processed for a lawful purpose directly related to an activity of the data controller;

b) the processing of the personal data is necessary for or directly related to that purpose; and

c) the personal data is adequate and reasonable but not excessive in relation to that purpose. The concerned Data Processor and Data Controller shall solemnly affirm through an affidavit that they have only processed adequate and reasonable but not excessive Personal Data in accordance with this Act, a record of which shall be kept for inspection and legal purposes.

Section 6

6.1

6.1 A data controller shall by written notice inform a data subject—

a) that personal data of the data subject is being collected by or on behalf of a Data Controller, and shall provide a description of the personal data to that data subject;

b) the legal basis for the processing of personal data and time duration for which data is likely to be processed and retained thereafter; the purposes for which the personal data is being or is to be collected and further processed;

c) of any information available to the data controller as to the source of that personal data;

d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data controller with any inquiries or complaints in respect of the personal data;

e) of the class of third parties to whom the data controller discloses or may disclose the personal data;

f) of the choices and means the data controller offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;

g) whether it is obligatory or voluntary for the data subject to supply the personal data; and

h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data.

We propose "written notice" should be replaced with "notice in writing both in hard copy and electronically together". This is to ensure that Data Subject can use such notice for evidentiary purposes later. Also, a sub-paragraph should be added to the effect "of the time period for which such data will be retained". Our proposed section is as under:

6.1 A data controller shall by a notice in writing transmitted both in hard copy and electronically to inform a data subject—

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

Controller, , and shall provide a description of the personal data to that data subject;

b) the legal basis for the processing of personal data and time duration for which data is likely to be processed and retained thereafter; the purposes for which the personal data is being or is to be collected and further processed;

c) of any information available to the data controller as to the source of that personal data;

d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data controller with any inquiries or complaints in respect of the personal data;

e) of the class of third parties to whom the data controller discloses or may disclose the personal data;

f) of the choices and means the data controller offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;

g) whether it is obligatory or voluntary for the data subject to supply the personal data;

h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data; and

i) of the time period for which such data will be retained.

6.2

6.2 The notice under sub-section (1) shall be given as soon as reasonably possible by the data controller—

a) when the data subject is first asked by the data controller to provide his personal data;

b) when the data controller first collects the personal data of the data subject; or

c) in any other case, before the data controller—

i. uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or

ii. discloses the personal data to a third party.

Section 6.2 (b) is unacceptable and should be omitted. It is an out-clause and defeats the purpose and safeguards of 6.1. Similarly, Section 6.2 (c) should be amended to exclude purposes other than for which data was collected. Our proposed section is as under:

6.2 The notice under sub-section (1) shall be given as soon as reasonably possible by the data controller—

a) when the data subject is first asked by the data controller to provide his personal data; or

b) in any other case, before the data controller discloses the personal data to a third party.

6.3

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

Section 6.3 – "applicable regional" should be added after national and before English. The words "where necessary" should be omitted. Our proposed section is as under:

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

Section 8

8.1

8.1 The Authority shall prescribe standards to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

8.1 The words "in accordance with international best practices" should be added after "standards". Our proposed section is as under:

8.1 The Authority shall prescribe standards, in accordance with international best practices, to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

8.2

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

a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

b) to the place or location where the personal data is stored;

c) to any security measures incorporated into any equipment in which the personal data is stored;

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

e) to the measures taken for ensuring the secure transfer of the personal data

We propose that "under strict liability of the law" should be added after "shall". Our proposed section is as under:

8.2 A data controller or processor shall under strict liability of the law, when collecting or processing personal data, take practical steps to protect the personal data in the terms mentioned under sub-section (1) by having regard—

a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

b) to the place or location where the personal data is stored;

c) to any security measures incorporated into any equipment in which the personal data is stored;

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

e) to the measures taken for ensuring the secure transfer of the personal data

8.3

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

We propose that "under strict liability of the law" should be added after "shall". Our proposed section is

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

8.4

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

8.4 After "independently" the words "jointly and severally liable with data controller " should be added. Our proposed section is as under:

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

Section 10

10.2

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

Section 10.2 the words "except where compliance with a request to such access or correction is refused under this Act" should be omitted. Our proposed clause is as under:

10.2 A data subject shall be given access to his personal data held by a data controller and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date.

Section 13

13.1

13.1 In the event of a personal data breach, data controller shall without undue delay and where reasonably possible, not beyond 72 hours of becoming aware of the personal data breach, notify the Authority in respect of the personal data breach except where the personal data breach is unlikely to result in a risk to the rights and freedoms of data subject.

We propose that the words "and the data subject" should be added after "Authority". The data subject has the right to know. The words "undue" and "and where reasonably possible" should be omitted. The words "except where the personal data breach is unlikely to result in a risk to the right and freedoms of data subject" should be omitted. This should be the call of the Data Subject and the Authority and not anyone else. Therefore, it should be omitted altogether.

13.1 In the event of a personal data breach, data controller shall without delay, not beyond 72 hours of becoming aware of the personal data breach, notify the Authority and data subject in respect of the personal data breach.

13.2

13.2 In the event of delay in notifying personal data breach beyond 72 hours, the personal data breach notification to the Authority shall be accompanied by reasons for the delay

We propose that the word "valid" should be added before "reasons" and "and Data Subject" should be added after "Authority". The words "under strict liability of the law" should be added after "shall". Our proposed section is as under:

13.2 In the event of delay in notifying personal data breach beyond 72 hours, the personal data breach notification to the Authority and data subject shall under strict liability of the law be accompanied by valid reasons for the delay

13.5

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

13.5 "under strict liability of the law" should be added after "shall".

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

Section 14

14.1

Critical personal data is not defined. It should be defined in the definitions section i.e. Section 2.

14.2

We propose that 14.2 should be omitted in entirety. The Federal Government should not have the power to exempt any personal data from the definition of either critical personal data or sensitive personal data.

14.3

The reference to subsection makes no sense here. It may be revisited.

Section 15

15.1

Critical personal data is not defined. It should be defined in the definitions section i.e. Section 2.

15.2

This section needs to be omitted in its entirety because it provides grounds for data localization for social media companies, intermediaries, tech giants, etc. offering cloud based services for Pakistani users and tech businesses to host data on their servers that are not locally hosted. This is similar to problematic provisions of Citizens Protection (from Online) Harm Rules 2020 where social media companies are asked to set up their offices in Islamabad. Additionally, it is unclear as to who the copy of personal data will be kept with and how. This would entail huge privacy implications.

Section 16

16.1

16.1 An individual is entitled to be informed by a data controller whether personal data of which that individual is the data subject is being processed by or on behalf of the data controller.

We propose that a new sentence "All Personal Data is the property of the Data Subject" should be added.

16.1 An individual is entitled to be informed by a data controller whether personal data of which that individual is the data subject is being processed by or on behalf of the data controller. All Personal Data is the property of the data subject.

16.2

16.2 A requestor may upon payment of a prescribed fee make a data access request in writing to the data controller—

a) for information of the data subject's personal data that is being processed by or on behalf of the data controller; and

b) to have communicated to him a copy of the personal data in an intelligible form.

We propose that the words "upon payment of prescribed fee" should be omitted. Our proposed section is as under:

16.2 A requestor may make a data access request in writing to the data controller—

a) for information of the data subject's personal data that is being processed by or on behalf of the data controller; and

b) to have communicated to him a copy of the personal data in an intelligible form.

16.3

16.3 should be omitted. It is unclear what a "single request" means in this case and in any event with the omission of prescribed fee, such a qualification becomes redundant.

Section 17

17.1

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

We propose that the words "and section 14," should be omitted. 30 days should be changed to 7 days.

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

17.3

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

We propose 14 days should be changed to 3 days. As the law stands it envisages 44 days *vis a vis* data access. This would leave the data subject at considerable disadvantage. It should be changed to three days in the interest of justice and fairness to data subject. We propose the following amended 17.3.

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

Section 18

18.1

18.1 A data controller may refuse to comply with a data access request under section 10 if—

a) the data controller is not supplied with such information as the data controller may reasonably require—

i. in order to satisfy itself as to the identity of the requestor; or

ii. where the requestor claims to be a relevant person, in order to satisfy itself—

a. as to the identity of the data subject in relation to whom the requestor claims to be the relevant person; and

b. that the requestor is the relevant person in relation to the data subject;

iii. to locate the personal data to which the data access request relates;

b) the data controller cannot comply with the data access request without disclosing personal data relating to another individual who can be identified from that information, unless—

i. that other individual has consented to the disclosure of the information to the requestor; or

ii. it is reasonable in all the circumstances to comply with the data access request without the consent of the other individual;

c) subject to subsection (3), any other data controller controls the processing of the personal data to which the data access request relates in such a way as to prohibit the first mentioned data controller from complying, whether in whole or in part, with the data access request;

d) providing access may constitute a violation of an order of a court;

e) providing access may disclose confidential information relating to business of the data controller; or

f) such access to personal data is regulated by another law.

We propose that (a) (c) (e) and (f) should be omitted. These cannot be considered valid or reasonable grounds to withhold requests. Our proposed section is as under:

18.1 A data controller may refuse to comply with a data access request under section 10 if—

a) the data controller cannot comply with the data access request without disclosing personal data relating to another individual who can be identified from that information, unless—

i. that other individual has consented to the disclosure of the information to the requestor; or

ii. it is reasonable in all the circumstances to comply with the data access request without the consent of the other individual;

b) providing access may constitute a violation of an order of a court.

Section 21

We propose that Section 21 should be omitted in entirety. There cannot be any circumstances under which a request of this nature should be denied by the Data Controller.

Section 22

22.1 b should be omitted along with Section 21 as a whole.

Section 24

24 (d) may be omitted. It is hard to foresee such circumstances.

Section 25

In general, we adopt gender inclusive language to the extent that "he" must be qualified with "or she".

25.2

25.2 Subsection (1) shall not apply where—

a) the data subject has given his consent;

b) the processing of personal data is necessary—

i. for the performance of a contract to which the data subject is a party;

ii. for the taking of steps at the request of the data subject with a view to entering a contract;

iii. for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by contract; or

iv. in order to protect the vital interests of the data subject; or

c) in such other cases as may be prescribed by the Federal Government upon recommendations of the Authority through publication in the Official Gazette

The words "by Data Subject's consent" should be added to 25.2 (b)(i) or it should be omitted altogether. 25.2(c) should be omitted. We propose the following section.

25.2 Subsection (1) shall not apply where—

a) the data subject has given his consent;

b) the processing of personal data is necessary—

i. for the performance of a contract to which the data subject is a party with data subject's consent;

ii. for the taking of steps at the request of the data subject with a view to entering a contract;

iii. for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by contract; or

iv. in order to protect the vital interests of the data subject

Section 28

It is hard to see the circumstances under which 28.1(b)i b) comes into action. It should be omitted to avoid confusion. The consent of the data subject is the cornerstone of this law.

Section 29

29 is unacceptable to us. Data Controller should comply with the provisions of Section 7 every time the Data Controller wants to process new data of the same Data Subject.

Section 31

Federal Government should not have the power to make additional exemptions. This should be left to the legislature as a fundamental right is involved. Section 31 should be omitted.

Section 32

As per international standards and global good practices, any statutory body established to safeguard a fundamental right has to be an autonomous and independent from the influence of governments and their allied departments. Therefore, we reject the proposal of establishing the Authority as a body corporate, and instead we recommend the establishment of an autonomous and independent Privacy and Data Commission through this Act. The commission should be empowered with administrative and financial autonomy, and the Federal Government should not have any influence on its decisions. This commission should be composed of civil society, private legal and IT experts appointed through a bi-partisan parliamentary committee only and no government employee should be part of it.

Without prejudice to our contention that there should be a Privacy and Data Protection Commission instead of an Authority and that the matter should be considered *de novo,* following are our amendments to Section 32 in its present form. We also feel that there is no need for ex-officio members in the said body and should be omitting. However here we are proceeding on the basis of present suggested composition.

We propose that the word "Authority" should be replaced with the word "Commission" throughout the Act. Furthermore Sections 37.2 and 38 should be omitted in entirety. The Commission should be completely autonomous and free of government control.

32.1

32.1 Within six months of coming into force of this Act, the Federal Government shall, by notification in the official Gazette, establish an Authority to be known as the Personal Data Protection Authority of Pakistan, to carry out the purposes of this Act.

Our changes to this are in line with our recommendations above.

32.1 Within six months of coming into force of this Act, the Federal Government shall, by notification in the official Gazette, establish an Commission to be known as the Commission For Privacy and Data Protection in Pakistan ("Commission"),, to carry out the purposes of this Act.

32.2

32.2 The Authority shall be a statutory corporate body having perpetual succession and a common seal, and may sue and be sued in its own name and, subject to and for the purposes of this Act, may enter into contracts and may acquire, purchase, take and hold moveable and immovable property of every description and may convey, assign, surrender, charge, mortgage, reassign, transfer or otherwise dispose of or deal with, any

moveable or immovable property or any interest vested in it and , shall enjoy operational and administrative autonomy, except as specifically provided for under this Act. The Authority shall be an autonomous body under the administrative control of the Federal government with its headquarters at Islamabad.

Our changes to this section include bringing it in line with the idea of commission which is independent and free of government influence.

32.2 The Commission shall be a statutory Commission, funded by the Federal Government, having perpetual succession and a common seal, and may sue and be sued in its own name and, subject to and for the purposes of this Act, may enter into contracts and may acquire, purchase, take and hold moveable and immovable property of every description and may convey, assign, surrender, charge, mortgage, reassign, transfer or otherwise dispose of or deal with, any moveable or immovable property or any interest vested in it and shall complete enjoy operational and administrative autonomy, except as specifically provided for under this Act. The Commission shall be a completely autonomous body with its headquarters at Islamabad.

32.4

32.4 The Authority shall consist of seven members, three of whom shall be an IT expert, a legal expert, a representative of civil society and a financial expert respectively, to be appointed by the Federal Government for a term of four years, who shall not be eligible for reappointment.

a) One ex-officio Member shall be a representative of the

i. Ministry of IT & Telecom

ii. Ministry of Defence

iii. Ministry of Interior

b) One regular Member (employee of the Authority) each from following sectors/areas:

i. Information and Communication Technology

ii. Financial

iii. Legal

iv. Civil Society

To make it a truly meritorious process and to keep the body free of partisan government influence , this section ought to be amended as under:

32.4 The Commission shall consist of seven members, comprising the following an IT member, two legal members, one financial member and three civil society members respectively, to be appointed by the Federal Government through an open merit policy and confirmed by a bipartisan parliamentary committee on data and privacy, for a term of four years, who shall not be eligible for reappointment.

32.6

32.6 The Authority shall be headed by a Chairman, who shall be nominated by the Federal Government from amongst the Seven Members.

We strongly feel that the chairman should not be appointed from the ex-officio members. Chairman's appointment by the Federal Government should also be confirmed by a bi partisan (treasury and opposition) parliamentary committee on data protection.

32.6 The Commission shall be headed by a Chairperson, who shall be appointed by the Federal Government from amongst the regular Members and confirmed by a bipartisan parliamentary committee on data protection and privacy.

32.9

We feel that pursuant to this section a lot of first-rate professionals will not opt to be the members. There should be no bar on business or professional engagements provided that Commission's work should come first.

Section 37

37.3

37.3 Three Members shall constitute a quorum for a meeting of the Authority

We feel that five members should constitute quorum and not three, in order to avoid the Authority's decisions to be dominated by *ex-officio* members (it must be stated here that we reject the very idea of having *ex-officio* members). Our proposed section is as under:

37.3 Five Members shall constitute a quorum for a meeting of the Commission.

Section 39s duplication

There are two Section 39s. The second one occurs after Section 40.

Section 41

41.1 Anyone who processes or cause to be processed, disseminates or discloses personal data in violation of any of the provisions of this Act shall be punished with fine up to fifteen million rupees and in case of a subsequent unlawful processing of personal data, the fine may be raised up to twenty five million,

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

We propose to add civil damages to the data subject as 41.3.

41.1 Anyone who processes or cause to be processed, disseminates or discloses personal data in violation of any of the provisions of this Act shall be punished with fine up to

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

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

41.3 The offender convicted under this section shall also pay direct, indirect and foreseeable damages to the data subject, whose personal data has been breached.

Sections 47 Duplication

There are two Section 47s and the first one is awkwardly named.

Conclusion

These amendments are the irreducible minimum, which will ensure that the statement of objects and reasons is faithfully abided by. We would once again stress that instead of an Authority, an independent Privacy and Data Protection Commission should be formed, without the inclusion of any ex-officio members from within any ministry or government department.

The government must realize the fact that the rationale behind Personal Data Protection Bill is to protect the personal data of Pakistani citizens, and will draw its powers from the Constitution's Article 14, which says, *"the dignity of man and, subject to law, the privacy of home, shall be inviolable".* However, the draft under consideration is an attempt to legalise the violability of natural and legal person's dignity and privacy of his or her personal data and the communication.

Personal data of an individual is his or her sole property and the state has the responsibility to protect it. However, the language of this proposed bill at several places, as notified in the above clause-by-clause analysis, suggests that the intention

of the state is *mala fide,* and instead the state wishes to integrate grey spaces by the use of subjective terminologies/language in the law for later times to be used as legal cushions to protect illegal collection and processing of the personal data of Pakistani citizens. This intention is also clear from the government's desire to establish an Authority, exactly on the lines of already existing weak and spineless regulators; including Pakistan Telecommunication Authority (PTA) and Pakistan Electronic Media Regulatory Authority (PEMRA), in the name of protection of personal data. Moreover, the representation of security institutions i.e. the Ministry of Interior and the Ministry of Defence is an alarming indication for the right to privacy. Such an Authority for the protection of the right to privacy is against the global democratic principles and good practices, and is unacceptable.

We urge the Government of Pakistan to set up Privacy Commission – an independent statutory body through this Act of the Parliament. Only this commission of experts will be able to provide and ensure an independent implementation of Personal Data Protection Bill in the country. This commission will have the sole responsibility to protect constitutional guarantees for the citizens and enable pro-people and pro-business Data Protection regime in Pakistan.

Contact Details:

For more information or any clarifications, please contact:

Email: info@bytesforall.pk

*This legal analysis is prepared by **Yasser Latif Hamdani** of the Honourable Society of Lincoln's Inn - Advocate High Court in collaboration with **Haroon Baloch**, Program Manager, Bytes for All, Pakistan. **Shahzad Ahmad**, the Country Director, Bytes For All reviewed the submission.*