FACULTY OF LAW
ZIAUDDIN UNIVERSITY

10th February, 2021

Consultation on the Personal Data Protection Bill, 2020

for the

Ministry of Information Technology & Telecommunications

[V.09.04.2020]

The Ziauddin Faculty of Law ('**ZFL**') is a premier legal education institute based in Karachi. It is the only law school in Pakistan to be members of both the International Association of Law Schools as well as the International Bar Association. Established in 2019, ZFL is already creating new standards of holistic legal education, practical learning and future-centric research projects.

The Centre for Law & Technology which functions under the auspices of ZFL is geared towards researching on matters of critical importance in the digital age. Headed by its Director, Mr. Aly Hassam Ul Haq (AHC), the Centre for Law & Technology has conducted a thorough assessment of the Personal Data Protection Bill ('**Bill**') for the purposes of consultation as requested by the Ministry of Information Technology & Telecommunication ('**Ministry**'). The assessment entailed a critical reading of the Bill with regard to the following considerations:

1. **The right to privacy:**

Where the right to privacy has historically related to the physical realm, the disruption caused by digitization and digital services has created the need for this right to extend to the digital realm- specifically with regard to the protection of personal data. The contemporary conceptualization of personal data is equatable to tangible possessions; the use of one's personal data ought to be in the knowledge and control of the person to whom that data relates. Consent, therefore, reigns supreme in matters of personal

data (with the exception of law enforcement related purposes, but even those matters are governed by the principles of necessity and proportionality).

2. Balancing interests:

Whereas the state and its institutions are more inclined towards having easier access to databases for the purposes of law enforcement and oversight, the individual beneficiaries of the Bill expect holistic protection of their personal data. The balancing of interests in light of the foregoing is quite a monumental task. On the one hand, Pakistan has unique security (relating to non-state actors) and transparency (relating to the government & official actors) issues, but on the other hand, those issues alone should not be the guiding factor for policies; policies guided by considering exceptions as the general rule are fundamentally misconstrued.

3. Net impact analysis:

The protection offered by the Bill is riddled with exceptions. A careful, considered analysis is conducted on the overall impact of the provisions of the Bill on the topic of personal data protection. The guiding philosophy behind data protection legislation, as mentioned hereinabove, is to allow data subjects to have knowledge and control of data relating to their person. Whilst the Bill provides for such knowledge and control, some of the exceptions (being far too broad in nature) render such knowledge and control redundant.

4. Executive overreach:

Whilst Data Protection Authorities worldwide have independence similar to that enjoyed by the judiciary, the Bill proposes a mechanism which is riddled with intervention/actual control by the Executive. Furthermore, ill-defined terms, lexical ambiguities, and arbitrary powers to make new exceptions effectively aim to legalize executive overreach. It is critically important to curb this notion to ensure stakeholders' confidence in the proposed legislation and subsequently, the Authority (once it is created).

5. International best practices:

While Pakistan is relatively fresh in the conversation on personal data protection, the international community has been concerned with it since as far back as the 1970s.

Having the added advantage of being able to research into those formative discussions on the topic, the Bill can potentially be a contemporary best-practice-oriented document, provided that the recommendations contained herein are incorporated and the Bill is amended accordingly.

6. Internal cohesion:

The Bill suffers from some internal inconsistencies which have been studied and highlighted. Usually, inconsistencies are removed via the interpretation of the law by the Courts or a legislative amendment. It is our position that these inconsistencies can be rectified prior to the promulgation of this Bill into an Act of Parliament to ensure that the judicial machinery is not burdened by the passing of this Act but rather is facilitated by the clarity that it offers. Clauses requiring correction have been duly recorded herein.

Summary of findings:

1. Three main guiding principles should be added to the Bill, namely:
    i. Proportionality
    ii. Necessity
    iii. Transparency & informed consent
2. The definition of sensitive personal data should be enhanced by including the data subject's political opinions and memberships, philosophical beliefs, and trade union memberships.
3. The Bill should include the provisions regarding the consent of the minor whose data is being/is to be processed.
4. The procedure of withdrawing consent should be defined in a simpler way, and its efficacy ought to be made clearer.
5. Terms such as 'vital interest' and 'legitimate interest' should be defined in the Bill to justify why consent is not necessary.
6. There must be clarity regarding the [class of] third parties to whom the data may be shared by the controller.

7. The provisions regarding the consent of the data subject should be defined in a simpler and clear way that without the consent of that data subject, the data cannot be processed.

8. The Bill should add provisions on data portability.

9. The Bill should add the requirement for informing data subjects of any breaches of their personal data.

10. Data controller satisfaction ought to be on a lower level of priority than the data subject in terms of data access, correction and/or withdrawal of consent requests.

11. The terms 'preventing' or 'detecting' crimes as a justification to access personal data seems to be overly-broad in their essence: fishing expeditions are effectively being legalized via this position.

12. Some provisions give unchecked power and authority to the Executive in terms of the arbitrary processing of data and of creating exemptions to the applicability of the substantive portions of this Bill.

13. There are some typographical errors found in the bill, as well as some conceptual confusion:

    a. 16.4, 18.1(c), 19.2 20.5, 21.1(e): conceptual error. A controller is one who makes decisions on processing a given data set. An entity which does not have this decision making authority cannot be defined as a controller. Furthermore, one controller's decisions on their data set cannot possibly prohibit the processing of the same data set which is held independently by another controller.
    b. 27.1(c): typographical error pertaining to citing section 23(2) which is irrelevant in the given context.
    c. 27.2: typographical error pertaining to the use of data 'controller' and 'processor' (they are not interchangeable).
    d. 29.1(a): typographical error which cites section 7 (which is irrelevant in the given context) instead of section 6 which contains the relevant information.

14. Data pertaining to statistical inferences, scientific or academic research, public health, trends and other useful data ought to be anonymized.

15. It is recommended that the scope of the exceptions mentioned in the Bill be limited significantly to be in conformity to the guiding principles. Furthermore, powers given to the Federal Government and the Authority to notify further exceptions/exemptions ought to be struck off.

In light of the foregoing, the detailed findings of the Centre for Law & Technology are elucidated hereinbelow:

Clause	Substantive Portion	Remarks
5.2	Notwithstanding subsection (1), a data controller may process personal data about a data subject if the processing is necessary: ... (d) in order to protect the vital interests of the data subject ... (f) for legitimate interests pursued by the data controller (g) for the exercise of any functions conferred on any person by or under any law ...	Subsection (1) of section 5 states that data shall not be processed without the consent of the data subject. Subsection (2) lays out the exceptions, i.e. circumstances where consent is not required for processing data. The most problematic exceptions are contained in 5.2(f) and (g), and a [relatively] less problematic exception lies in 5.2 (d) 5.2(d): the protection of a person's vital interests is the mandate of the Police and Security forces. However, if data processing is necessary for the protection of a data subject's vital interests, the decision-making ought to be transparent, and ought to follow strict principles of proportionality and necessity.

		5.2(f): 'Legitimate Interest' of the data controller is not defined. Controller's discretion must be curbed and consent must be given precedence over such discretion. 5.2(g): This provision is much too broad and open-ended. It suggests that any such person on whom the law confers a function/duty may request *any* data controller to process personal data on their request in order to fulfil that function, *without the knowledge and/or consent of the data subject.*
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 ... (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;	6.1 (a) The provision reads that the notice must be sent when personal data "is being collected". This is problematic on 2 counts: 1. In effect, consent is not required for the collection of data 2. Collection of data falls under the definition of 'Processing' [see: 2(f)] Therefore, it is recommended that consent precedes the collection of personal data, and the consent 'notice' or 'form' should contain all necessary information to obtain informed consent (i.e. the information contained in the notice to the data subject ought to be given to them prior to collection, and as a basis for getting the data subject's consent).

	e) of the class of third parties to whom the data controller discloses or may disclose the personal data …	6.1(d): The notice contains information on the rights available to the data subject, but omits informing the data subject of their right to erasure of data. The presence of this right must also be communicated to the data subject within the notice. 6.1(e) There seems to be some ambiguity regarding the status of [a class of] 3rd parties with whom data may be shared by the controller. The ambiguity may be removed if clarity can be achieved on the following questions: 1. Will these 3rd parties be compelled to erase data if an erasure request is sent to the initial data controller? 2. Will the status of these 3rd parties change to 'data controller' when personal data is shared with them? a. Would the 3rd parties- by virtue of this status change (or otherwise) - be required to adhere to the requirements of information sharing with the data subject as is the responsibility of data controllers? - Since, in effect, these 3rd parties will be processing data and should be considered either processors or controllers, depending on the nature of their work. 3. Are 3rd parties further allowed to share personal data with the same class of 3rd parties once they have received the personal data?

		Furthermore, in conjunction with the foregoing, the 'class' of 3rd parties is quite a broad classification. For instance, if the 'class' of 3rd parties are advertisers/marketing concerns, there may be hundreds (if not thousands) of such concerns in the applicable jurisdiction. Sharing personal data with such a large set of concerns dilutes the purpose and consent-based control of personal data by data subjects.
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	The language suggests that the mere serving of the notice to the data subject is sufficient for the data controller to begin processing personal data and/or to begin disseminating that data to 3rd parties. Furthermore, the language also suggests that the data may be processed for a purpose other than that on the basis of which consent was obtained upon the mere serving of the notice to the data subject. 6.2(b) stipulates that the notice be sent to the data subject after the first collection of personal data. However, *consent* is required for the initial collection of personal data (since 'collection' falls under the definition of 'processing') - but this aspect is apparently disregarded in 6.2(b).

	which the personal data was collected; or ii. discloses the personal data to a third party.	It ought to be made explicitly clear that data cannot be collected without the consent of the data subject, along with the data subject being informed (in addition to their rights) as to the nature of data being collected, the purposes it is being collected for, how it will be stored, how it will be processed, with whom will it be shared (if at all), and how long it may be retained for.
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.	These prescribed standards must comply with international best practices, and the onus should be on data controllers to ensure all resources are present prior to engaging in data processing. This standard ought to be codified within this section.
8.2	A data controller or processor shall, when collecting or processing personal data, take practical steps to protect the personal data...	'Practical' steps is too loose a term; such steps could easily be justified without being reasonable and/or adequate. Therefore, it is recommended that the word 'practical' be substituted with 'adequate'.
9	9.1 The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.	The phrasing of subsection (1) is quite clear- i.e. data shall only be retained for as long as it is *necessary* to retain it for the specified purposes. However, subsection (2) dilutes the impact of the first subsection due to the

	9.2 It shall be the duty of a data controller to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.	phrase 'reasonable steps'. If data is to be erased and the standard of necessity is to be maintained, then all conceivable steps ought to be taken to *ensure* (in the true sense of the word) the deletion of personal data by the data controller.
10	10.1 A data controller shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed. 10.2 A data subject shall be given access to his personal data held by a data controller and 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.	Subsection (2) of section 10 dilutes the essence of subsection (1): personal data ought to be up to date, accurate, complete and not misleading, however, the same cannot be accomplished if the data subject is refused access/correction to the data. The possibility of refusal has been codified in subsection (2). Granted, such a refusal [to access or correction] is governed by- *inter alia*- sections 18 and 21, the grounds for refusal are too broad in nature for this provision to be reasonable, for instance, a ground for refusing access is [per section 18.1(e)] 'providing access may disclose confidential information relating to business of the data controller'. Furthermore, a correction request may also be refused if [per 21.1(c)] 'the data controller is not satisfied that the personal data to which the data correction request

		relates is inaccurate, incomplete, misleading or not up-to-date'. It is recommended that this discretion should not lie with the controller but rather to the data subject to whom the personal data pertains. Following this, however, the onus/liability for the veracity/accuracy of data supplied with a correction request shall lie on the data subject, and a penal measure should be imposed for false, inaccurate or misleading information. Personal data pertaining to a data subject ought to be free of encumbrances and should be available for access, rectification and deletion easily (and without incurred cost).
11	11.1 A data controller shall keep and maintain a record of any application, notice, request or any other information relating to personal data that has been or is being processed by him. 11.2 The Authority may determine the manner and form in which the record is to be maintained.	There is an ambiguity in the effect of this provision, i.e., how are such records to be balanced against the right to erasure? [see section 27]. There is also another conflict with the principle of necessity as elucidated in section 9 (i.e. only retaining data for as long as it is necessary for the defined purposes). It could be possible that the maintenance of records, applications and notices contain enough information within them to be construed as personal data. This is

		also the case with maintaining records as per section 13. This seems to be an internal inconsistency within the draft bill.
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.	1. Notifications of data breaches are to be sent to the Authority - nothing contained in the Bill suggests that the data subject will be informed of any data breach. It is recommended that all reasonable and practical steps be taken to inform data subjects of data breaches as well. 2. Notifications do not need to be sent to the Authority if the data breach 'is unlikely to result in a risk to the rights and freedoms of [the] data subject'. The term 'unlikely' is discretionary and vague. It is submitted that controllers and processors have a vested economic and reputational interest in appearing secure and so the likelihood of them understating the extent of data breaches is quite high. Furthermore, if a data breach is not reported under the garb of it being 'unlikely' to affect the data subject, it may be wrongly construed as such by the data controller. It is recommended that all data breaches be communicated both to the Authority as well as to data subjects, along with measures taken to mitigate the breach and/or consequences thereof.

		Moreover, it is recommended that 72 hours be the maximum cap to declare a breach where it has been ascertained, and to add details of the breach as soon as possible after the discovery (following an internal investigation) of the details of the breach.
14	Provided that if personal data is required to be transferred to any system located beyond territories of Pakistan or system that is not under the direct control of any of the governments in Pakistan, it shall be ensured that the country where the data is being transferred offers personal data protection at least equivalent to the protection provided under this Act and the data so transferred shall be processed in accordance with this Act and, where applicable, the consent given by the data subject. 14.1 Critical personal data shall only be processed in a server or data centre located in Pakistan.	'Critical personal data' is to be classified [per section 2(o)] by the Authority with the approval of the Federal Government. It is submitted that the use and placement of the phrase 'critical personal data' in the Bill allows for fundamental exceptions to be made in terms of which data is classified as critical personal data, which will effectively bar certain sets of data from leaving the territorial jurisdiction of Pakistan. Data localization [see section 15] is not strictly required for data protection, and it is an internationally-settled notion that fewer copies of personal data translates into a lesser likelihood of data breaches. Furthermore, given the government-access-friendly nature of the Bill, data localization may serve as a deterrent for foreign companies and/or foreign data subjects to do business in Pakistan since there is no real guarantee that the personal data will be kept secure in the absence of a proper legal basis to access that data. [Since all personal data is

	... 14.3 Nothing contained in sub-section (3) shall apply to sensitive personal data.	accessible for 'detecting', 'investigating' and even 'apprehending' potential (or potentially future) crimes and criminals. Such a mechanism presupposes the guilt of the concerned party insofar as the sanctity of their data is concerned, i.e. no strict legal procedure or court order is necessary for law enforcement agencies to access personal data databases. Furthermore, section 14.3 has a typographical error since it is- in essence- referring to itself. This section (i.e. 14) needs to be re-numbered correctly.
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 ...	The requirement to submit a fee for an access request is disproportionate and goes against the spirit of personal data protection and the element of control which data subjects have over their personal data. Furthermore, it is recommended that a data portability provision be added to the Bill, i.e. adhering to common technical standards to facilitate the transfer of personal data from one controller to another.
18.1 (a) & (b)	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	Information required to 'locate' personal data: this effectively allows data controllers to excuse themselves from an access request on the basis of being unable to locate where the data is stored. Such storage and referencing ought to be the

	controller may reasonably require: ... 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	responsibility of the controller to monitor and log for ease of access. However, it *may* be that this is not the intended effect, in which case it is recommended to limit the scope of this provision to have the effect that enough identifying markers ought to be given to the controller by the subject to enable the controller to locate the data via a search (or tabulated & referenced storage method, as the case may be). Moreover, where data relates to another individual, the access request should not be refused, but rather the data ought to be separated from the data of the other person and sent to the requestor. Alternatively, the other person's data could be anonymised before sending it to the requestor. Under no circumstances should the consent of a data subject be *assumed*, even if such an assumption is meant to be gauged by the standard of 'reasonability'. Granted, added protection is offered by section 18 subsection (2), but such protection is cosmetic in nature and does not adequately protect the rights and interests of data subjects.

18.1 (c)	A data controller may refuse to comply with a data access request under section 10 if: (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	This seems to be a conceptual error - a controller is an entity who makes decisions on how personal data is to be processed. One controller's decisions are mutually exclusive of another controller's decisions. Even where data sets converge wholly or in part, one controller's processing actions cannot conceivably 'prohibit' another controller from exercising their functions as a controller on the data set in their possession.
18.1 (e) & (f)	A data controller may refuse to comply with a data access request under section 10 if: (e) providing access may disclose confidential information relating to business of the data controller (f) such access to personal data is regulated by another law.	The business of the data controller and the data subjects' personal data are mutually exclusive paradigms. If disclosing the personal data of a data subject discloses information about the business, i.e. which personal data they collect, how that personal data is processed, with whom is that personal data is shared, etc., the data subject should not be refused their right to access (and correction, and erasure) to protect the business model of the data controller. This significantly goes against the spirit of data protection and enhanced data subject control over their personal data. This provision, in effect, can allow controllers to excuse themselves from compliance on the basis of the

		'confidential' information which can be extrapolated about their business from the personal data they collect and how it is processed. It is recommended that the access to personal data be regulated only according to the special law (the current Bill) on data protection, which shall trump all other laws currently in force (as stipulated in section 49). It is recommended that both these clauses are removed from the Bill (i.e. 18.1 (e) & (f)).
20.5	Where a data controller is requested to correct personal data … and the personal data is being processed by another data controller that is in a better position to respond to the data correction request (a) the first-mentioned data controller shall immediately transfer the data correction request to such data controller, and notify the requestor of this fact …	The mention of multiple controllers is rather concerning. First and foremost, the same conceptual error is manifest as was in 18.1(c), i.e. a controller is an entity who makes decisions on how personal data is to be processed. One controller's decisions are mutually exclusive of another controller's decisions. Even where data sets converge wholly or in part, a request for correction ought to be handled by the controller who receives it, whilst making recommendations to the subject as to which other controller to make the same request to. However, this puts an added burden on controllers, i.e. controllers will, in order to

		be compliant, need to have actual and up-to-date knowledge of which 'other' controller is processing data of an overlapping data subject between the two controllers. This burden already exists in effect, according to the language of the Bill. Notwithstanding the above, it is also quite unclear what being in 'a better position' means for a controller.
21.1	A data controller may refuse to comply with a data correction request under section 20 if: ... (c) the data controller is not satisfied that the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up-to-date ... (e) subject to subsection (2), any other data controller controls the processing of the personal data to which the data correction request relates in such a way as to prohibit the first-mentioned data controller from complying, whether in whole	21.1 (c): the controller's 'satisfaction' ought to be on a lower level of priority than the data subjects since the general presumption is that data subjects know more about their own personal data than the controllers do. Therefore, the onus ought to be on the data subject to provide accurate and up-to-date information, coupled with a penalty for submitting false, outdated or misleading information. 21.1 (e): This seems to be a conceptual error - a controller is an entity who makes decisions on how personal data is to be processed. One controller's decisions are mutually exclusive of another controller's decisions. Even where data sets converge wholly or in part, one controller's processing actions cannot conceivably 'prohibit' another controller from

	or in part, with the data correction request	exercising their functions as a controller on the data set in their possession.
24	Notwithstanding section 7, personal data of a data subject may be disclosed by a data controller for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances: b) the disclosure: i. is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations (c) the data controller acted in the reasonable belief that he had in law the right to disclose the personal data to the other person; or d) the data controller acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the	This clause is highly problematic: it essentially reverses the protection offered by sections 5, 6 & 7, making the purpose-based processing model redundant in its entirety. 24 b(ii): 'preventing' or 'detecting' crimes as a justification to access personal data seem to be overly-broad in their essence; fishing expeditions are effectively being legalized via this provision. 24 (c) & (d) ought to be removed outright. Under no circumstances should a data controller assume their legal rights or consent of the data subject. 24 (e) gives the Authority overly-broad (and unchecked) powers to create a list of justifiable circumstances which may be used as a basis for disclosure under the garb of public interest. There is effectively nothing stopping the Authority from creating disproportional justifications. It is imperative that the Authority be saved from political hijacking, i.e. it is commonplace for institutional policies to be defined by the political landscape of the hour; creating overly-broad loopholes for

	disclosing of the personal data and the circumstances of such disclosure; or e) the disclosure was justified as being in the public interest in circumstances as determined by the Authority in advance of the disclosure.	the Authority under the garb of 'public interest' creates room for political hijacking. Therefore, it is recommended that a check-and-balance system be appended with this power to create a list of justifications with respect to disclosure.
25.1	Subject to subsection (2), a data subject may, at any time by notice in writing to a data controller, referred to as the "data subject notice", require the data controller at the end of such period as is reasonable in the circumstances, to: a) cease the processing of or processing for a specified purpose or in a specified manner; or b) not begin the processing of or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject if, based on reasons to be stated by him:	This section essentially renders the requirement for consent prior to the processing of personal data, redundant. (or vice versa: with section 23 rendering section 25 redundant). Furthermore, it appears that if a data subject sends a withdrawal of consent notice [see section 23], the instant provision would be deemed ineffective and the data controller would be compelled to comply and cease all processing. However, it is pertinent to note that perhaps some data is being processed without consent (since it may have fallen into one of the exemptions), and so this provision could be attracted. In any case, the requirement to satisfy the controller as to the likelihood of unwarranted harm and/or distress is

	i. the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or a relevant person; and ii. the damage or distress is or would be unwarranted.	unfounded and contravenes the spirit of data protection. Consent ought to be the basis of all data protection by *private* actors. There should exist exemptions for public actors, but only insofar as is necessary for the investigation of a crime, of maintaining national databases, of maintaining registers and public records, and other critical functions of a state.
25.2	Subsection (1) shall not apply where: … (b) the processing of personal data is necessary: … iii. for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by contract .. (c) in such other cases as may be prescribed by the Federal Government upon recommendations of the Authority through publication in the Official Gazette	This provision grants too much discretionary power to the Executive in terms of creating exceptions within which topic area, data subject notices will have no effect. This position is further fortified by the fact that any notification issued by the Federal Government or any Ordinance or Law passed by the relevant authority shall enable further exceptions to be created. This fuels distrust by the data subject in the machinery responsible for protecting their personal data.

25.3	The data controller shall, within twenty-one days from the date of receipt of the data subject notice under subsection (1), give the data subject a written notice: a) stating that he has complied or intends to comply with the data subject notice; or b) stating his reasons for regarding the data subject notice as unjustified, or to any extent unjustified, and the extent, if any, to which he has complied or intends to comply with it.	Although the controller must respond within 21 days, there is no deadline for compliance. It is recommended that compliance is done within 21 days of receipt of the data subject notice, or if it cannot be complied with, then sending a notice with reasons as to why compliance is not done. Furthermore, the 14-day requirement of compliance after the initial 21-day period ought to be added here.
26	Foreign data subject shall have all his rights, if any provided under the laws of the country or territory where the foreign data has been collected or data subject resides in so far as consistent with this Act.	There ought to be a special office which is responsible for creating 'data pockets' with enhanced protection in order to attract business from- say- the EU. The General Data Protection Regulation only allows for cross-border transfers of data where the jurisdiction of the transferee has equal or more protection than the GDPR offers. However, it is important to note that the GDPR requires local *laws* to offer equal or more protection than the GDPR,

		therefore, perhaps the powers conferred to the Authority by this piece of legislation should also contain a provision allowing the authority to formulate enhanced protection rules (which are allowed by the Parliament to go beyond the scope of the parent Act) for particular jurisdictions. Alternatively, Parliament could promulgate jurisdiction-specific data protection laws so Pakistan can do more business with the EU and other international jurisdictions.
27.1	The data subject shall have the right to obtain from the data controller the erasure of personal data concerning him without undue delay and the data controller shall have the obligation to erase personal data within a period of 14 days where one or more of the following condition applies: … b) the data subject withdraws consent on which the processing is based in accordance with section 23 (1) and where there is no other legal ground for the processing; or	27.1(b) stipulates that the withdrawal of consent in itself is not sufficient as a grounds for erasure of data- it adds the requirement that the personal data has no other legal ground for processing. It is recommended that such 'legal grounds' be limited to adherence to an order of the Court or the discharge of a statutory function; that too insofar as is strictly necessary. Furthermore, in 27.1(c), the section quoted (i.e. subsection (2) of section 23) is irrelevant. There must be a typographical error within this clause.

	c) the data subject objects to the processing pursuant to sub-section (2) of section 23;	
27.2	Where the data controller has made the personal data public and is obliged pursuant to subsection (1) to erase the personal data, the data controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform data processors which are processing the personal data that the data subject has requested the erasure by such data controllers of any links to, or copy or replication of, those personal data.	Clarification is required in terms of the following: 1. On what grounds can the data be made public without it constituting a breach by the controller? 2. What are the benchmarks for these cost considerations? Data controllers have a vested interest in not incurring costs in order to ensure data erasure- this provision may result in a situation where even (relatively) small costs may be used as a basis for avoiding completing an erasure of data exercise. Furthermore, there is a phrasing error in this section. At one point the data processor is mentioned, and in the very same sentence, reference is made to a data controller.
27.3	Subsections (1) and (2) shall not apply to the extent that processing is necessary: a) for exercising the right of freedom of expression and information ...	27.3(a) It is unclear what the meaning, effect and basis for subsection (a) is. Whose right of freedom of expression and information can be affected by a data subject's personal data? It is recommended that this provision contain a public-private distinction, along with properly defining which data is allowed to

	c) for reasons of public interest in the area of public health d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in subsection (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing	be made public (for instance, criminal records or records pertaining to public servants) 27.3(c) & (d) health data and every other personal and sensitive data which is being stored/archived/studied ought to be anonymized. This will ensure the privacy of data subjects whilst simultaneously allowing for research and statistical inferences to be made.
28.1	Subject to subsection (2) of section 5, a data controller shall not process any sensitive personal data of a data subject except in accordance with the following conditions: ... b) the processing is necessary: ... iii. in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld	Consent is meant to be free, informed and unambiguous. The discretion to give (or withhold) consent lies with the data subject; the decision of the data subject ought not to be interpreted as reasonable or unreasonable. Furthermore, the proportionality test ought to be introduced in this provision; for in the case where a person's vital interests are in jeopardy, perhaps processing anonymized or pseudonymised data would be appropriate and adequate.
29.1	Where a data controller—	It seems there may be a typographical error in this section, i.e. section 7 pertains

	a) has complied with the requirements of this Act in respect of the collection of personal data from the data subject, referred to as the "first collection"; and on any subsequent occasion again collects personal data from that data subject, referred to as the "subsequent collection", the data controller shall not be required to comply with the requirements of section 7 in respect of the subsequent collection if— i. to comply with those provisions in respect of that subsequent collection would be to repeat, in the same circumstances, what was done to comply with that principle in respect of the first collection; and ii. not more than twelve months have elapsed between the first collection and the subsequent collection.	to non-disclosure of data. We are of the view that perhaps section 6 (the requirement to send data subject notices) is more fitting, given the language of the provision.
30.2	Subject to section [28] and critical personal data, personal data:	Sections 5, 6, 7 and 8(2) contain the substantive protection of personal data. Creating exemptions to these provisions

	a) processed for i. the prevention or detection of crime or for the purpose of investigations; ii. the apprehension or prosecution of offenders; or iii. the assessment or collection of any tax or duty or any other imposition of a similar nature by the relevant authority shall be exempted from sections 5, 6, 7 and subsection (2) of section 8 of this Act and such other related provisions of this Act as may be prescribed by the Authority for specific purposes; (b) processed in relation to information of the physical or mental health of a data subject shall be exempted from subsection (2) of section 8 and other related provisions of this Act of which the application of the provisions to the data subject would be likely to cause serious harm to	may be problematic, specifically in the case of: i. The prevention or detection of crime: this provision is much too fishing-expedition-friendly. It circumvents the requirement for due process to access data and that LEAs and Regulatory Authorities would be allowed to legally access and process personal data without a valid cause or basis. ii. The *assessment* of tax or duty or any other imposition of a similar nature: for the same reasons stated above. It is recommended that the scope of these exceptions be limited, especially since there is no applicability of the requirement to send a data subject notice and there is no bar to the disclosure of the personal data (see section 7). Furthermore, it is absurd that there are no security standards applicable on the data collected/processed for these exemptions (see 8.2). In clear categorical terms, the beneficiaries of these exemptions do not need to care for (*inter alia*): 1. Data security or any harm that may befall the data subject due to misuse, modification or disclosure of the data 2. Any security measures to ensure the data is not misused/accessed/disclosed

	the physical or mental health of the data subject or any other individual; ... f) processed only for journalistic, literary or artistic purposes shall be exempted from sections 5, 6, 7, 8, 9, 10, 11 and other related provisions of this Act, provided that— i. the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material;	3. The veracity/accuracy/truthfulness of such data 4. Disclosure of data, i.e. they are under no obligation to keep the data in their own possession alone. It is pertinent to secure data as per the requirements stipulated in section 8, as well as ancillary requirements in sections 5, 6 and 7. Creating exceptions to these fundamental protections renders the spirit of data protection meaningless and redundant and ought to be revisited. It is recommended that *specific* exceptions be granted for LEAs and national databases, however, data security ought not to be an exception. Moreover, the most problematic section of the Bill is 30.2 (f). The exemptions created therein for journalistic, artistic and literary purposes without regard to authenticity, the non-disclosure requirement, or, in essence, any of the substantive protection clauses in this Bill, have essentially rendered the fundamentals of this piece of legislation toothless and redundant.
31	31.1 The Federal Government may, upon the recommendation of the Authority, by order published	Section 31 is overly broad and amounts to an overreach of powers to promulgate delegated legislation. There is no apparent check-and-balance mechanism to oversee

	in the official Gazette exempt the application of any provision of this Act to any data controller or class of data controller.	which exemptions are notified by the Federal Government.
34	(2) In particular and without prejudice to the generality of the foregoing power, the Authority shall ... (f) Formulate a Licensing Framework for Data Controllers and Data Processors on Personal Data Protection in Pakistan	Licensing in terms of data protection is, in effect, a bar to the proper implementation of personal data protection laws. It may result in a monopolization of controllers and processors, which defeats the purpose and will add to backlog problems in the future.
39	Co-operation with International organizations.—The Authority may, subject to the prior approval of the Federal Government, co-operate with any foreign authority or international organization in the field of data protection / data security / data theft / unlawfully data transfer on the terms and conditions of any program or agreement for co-operation to which such authority or organization is a party, or pursuant to any other international	There is a numbering error in the Bill - after 38, 39, 40, section 39 (the number) is repeated again. The second section 39 is the one reproduced here. It is recommended that this be consolidated with the proposed office responsible for creating jurisdiction-based protective arrangements in order to do business with foreign jurisdictions where data protection laws require that if personal data is being transferred abroad, then the receiving jurisdiction's legislative protection of data ought to be equal to, or more than the protection offered by the sending jurisdiction's laws. (Please see comments on section 26).

	agreement made or after the commencement of this Act.	

After an examination of the analysis and discussion contained herein, it is pertinent to mention that there are significant aspects of personal data protection which have been omitted from the Bill altogether. It is quite interesting to observe that a few of the recommendations to follow were in fact a part of the 2018 draft Bill, but have been removed in the 2020 draft Bill. Nevertheless, our recommendations for addition are as follows:

A. Enhancing the definition of sensitive personal data to include the data subjects' political opinions and memberships, philosophical beliefs, trade union memberships, commission of offences until a conviction is secured, and genetic data.

B. Adding provisions on consent for minors whose data is being/is to be processed.

C. Adding provisions on data portability, i.e. adhering to common technical standards to facilitate the transfer of personal data from one controller to another.

D. Adding the requirement of a data protection officer to be deputed by data controllers who are internal employees/associates of the controller but function independently to ensure that the controller is in compliance with data protection legislation.

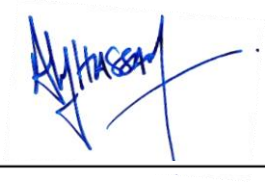
E. Adding the requirement for informing data subjects of any breaches of their data. Currently, only the Authority needs to be intimated; the data subject is the more relevant party to be informed so that they may take such steps as are necessary to counter the exposure resulting from the breach.

F. Adding the following as salient guiding principles on personal data protection:

a. Transparency & Informed Consent – collection and processing ought to be undertaken with complete transparency and absolute knowledge (and consent based thereupon) of the data subject.
b. Purpose & Storage Limitation (necessity) – data ought to be collected for a specified purpose and only stored for so long as is strictly necessary for the defined purposes.
c. Data Minimization (proportionality) – only such data ought to be collected and processed as is strictly necessary for the defined purposes.

The ZFL Centre for Law & Technology is honoured to be able to contribute to the discussion and would be happy to further assist the Ministry on the topic. We hope that the recommendations and analysis contained herein prove to be fruitful in your deliberations, and we look forward to seeing a balanced and well-drafted Data Protection Act, duly passed by the Parliament.

Sincerely,



Aly Hassam Ul Haq
LL.M., Law & Technology (Netherlands)
Advocate, High Courts of Pakistan
Director, Centre for Law & Technology

Alishba Fazal-Ur-Rehman
Student Research Associate

Areeba Iqbal Qureshi
Student Research Associate

10th February, 2021