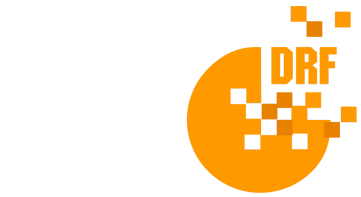

PERSONAL DATA PROTECTION BILL 2020

Civil Society Submission to the Ministry of Information Technology and Telecommunications

May 5, 2020

Submission by **Digital Rights Foundation**

About: Digital Rights Foundation

The Digital Rights Foundation (DRF), founded in 2012, is a research-oriented and advocacy not-for-profit organization working on issues of online freedom of expression, the right to privacy and online harassment against women and gender minorities. DRF aims to make the internet a safe and accessible space for all.
www.digitalrightsfoundation.pk

History of Data Protection Legislation in Pakistan

According to the UN, 107 countries across the world have enacted data protection and privacy legislation.[1] In order to ensure the fundamental rights of its citizens and compliance with international human rights standards, Pakistan has also taken steps to enact a personal data protection law in Pakistan. Article 14 of the Constitution of Pakistan guarantees the Right to Privacy, however serious efforts to introduce a law were first taken in 2018 (though a draft Bill was put forward in 2005 but was deemed too weak) when the Ministry of Information Technology and Telecommunication (MOITT) introduced a draft Personal Data Protection Bill in July 2018 and invited comments from the public. The Bill lauded as a good first step, however, suffered from serious issues in terms of scope as it restricted the definition of personal data to "commercial transactions", limiting its applicability to government-held data, and the proposed Data Protection Commission was not sufficiently independent in its functions and composition.[2]

A second iteration of the Bill was shared by the Ministry in October 2018, with slight improvements in terms of definitions but many of the same concerns remained especially when compared to international best practices such as the General Data Protection Regulation (GDPR). There was little headway by the MOIT since despite appeals from civil society[3] and being taken up by bodies such as the Senate Standing Committee on Human Rights.[4] The third draft of the Personal Data Protection Bill (referred henceforth as the "Bill"), was put forward by Ministry in April 2020[5].

Executive Summary

We appreciate the efforts by the MOITT in making data protection and privacy of citizens a priority. Furthermore, we welcome the consultative process adopted by the Ministry. However, we hope that during a time when the entire world, including Pakistan, is under lockdown and reeling from the economic, social and public health implications of the COVID-19 pandemic, that such important legislation will not be passed hastily and without the opportunity for an inclusive and open consultative process.

---

[1] Data Protection and Privacy Legislation Worldwide Data Protection and Privacy Legislation Worldwide, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.
[2] "Comments on the Personal Data Protection Bill, 2018 - Joint Submission by Digital Rights Foundation and Privacy International", https://digitalrightsfoundation.pk/wp-content/uploads/2018/08/DP-Comments-Brief-Final-8.8.18-1.pdf.
[3] "MPs, lawyers talk of implementing legislation protecting fundamental rights", 2019, https://www.thenews.com.pk/print/463677-mps-lawyers-talk-of-implementing-legislation-protecting-fundamental-rights.
[4] "Hearing at the Senate Standing Committee on Human Rights regarding Privacy and Harassment", https://digitalrightsfoundation.pk/hearing-at-the-senate-standing-committee-on-human-rights-regarding-privacy-and-harassment/.
[5] A copy of the 2020 Bill can be found here: https://www.moitt.gov.pk/SiteImage/Misc/files/Personal%20Data%20Protection%20Bill%202020(3).pdf.

The new 2020 Personal Data Protection Bill, while a better version in comparison to the drafts issued in 2018, still does not fully capture the data protection needs of people in Pakistan. The most prominent issue we see with the draft is the exemption-making and wide-ranging powers given to the Federal Government, in particular under Sections 31 and 38 which risk undermining the protections afforded under the Act. Government bodies collect and process vast amounts of personal data and the obligations in the Act must extend to them and the Government should not be able to introduce further exemptions without proper scrutiny and safeguards. Additionally, the independence of the Personal Data Protection Authority of Pakistan needs to be ensured, by limiting the powers of the Federal Government to appoint members and approve rules made by the Authority (Section 48).

The need for and reliance on technology has and will drastically increase during the COVID-19 pandemic and in a post-Coronavirus world where we will see a predominantly offline world transform into an online world. Access to online platforms of communication, healthcare, education and business is no longer a luxury. In the midst of all this, the need for protection of our personal data is essential more than ever.

Our primary recommendations to the Ministry are (please find our detailed analysis on page 10:

1. Definitions of terms such as “Public Interest” and “Critical Personal Data” should be explicitly defined under the Act;
2. The definition of “Sensitive Personal Data” should be expanded to include categories such as “membership of a trade union” and “philosophical and/or religion beliefs”;
3. Implementation of the Act should be on a progressive basis to ensure a balance between rights protection and a grace period for data controllers to ensure compliance;
4. Clearer language regarding scope and jurisdiction of the Act;
5. Mandatory requirements for obtaining consent should be expanded to include information on intention to transfer of personal data to a third country and the level of protection provided, the existence profiling for targeted purpose, and the existence of automated decision-making;
6. The Act should develop a higher consent standard for personal data of children and young adults below the age of majority;
7. Clearer and minimum requirements for security measures for data controllers should be laid down in the Act;
8. Data localisation measures introduced for cross-border personal data flows should be seriously revised in light of international best practices;
9. Procedure for withdrawal of consent should be simplified to ensure that it is as easy for the data subject to withdraw consent as it is to give it;
10. Rights of data subjects such as the right to data portability, right to information related to profiling and automated decision-making, and right to compensation should be explicitly included in the Act;
11. Powers of the Federal Government to make exemptions under Section 31 be removed;
12. Safeguards should be included to ensure independence of the Data Protection Authority;
13. Powers of the Federal Government to issue policy directives under Section 38 should be removed.

Comparison between the Personal Data Protection Bill 2018 (October) and the 2020 Draft Bill

In this section we will comparing some of the recommendations we made in their policy brief for the second version of the Bill in 2018 to the current 2020 version:

Recommendations in Policy Brief by Privacy International and Digital Rights Foundation on 2018 PDPB	PDPB 2020 (V.09.04.2020)
Chapter 1 - Preliminary	**Chapter 1 - Preliminary**
S.2 (d) - Data Controller: any person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor.	**S.2 (c) - Data Controller**: any natural or legal person or the government, who either alone or jointly has the authority to make a decision on the collection, obtaining, usage or disclosure of personal data.;
S. 2 (e) - Data Processor: in relation to personal data, means any person, other than employee of the data controller, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes.	**S. 2 (d) - Data Processor:** means a natural or legal person or the government who alone or in conjunction with other(s) processes data on behalf of the data controller.
Anonymized Data has not been defined	**S.2 (e) - Anonymized Data:** means information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable
Relevant Person has not been defined	**S.2 (i) - Relevant person** in relation to a data subject means (a) in the case of a data subject who is below the age of 18 years, the parent or a guardian appointed by a court of competent jurisdiction; (b) in case of a data subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs; or (c) a person authorized by the data subject to make a data access and/or data correction request.

S.2(n) - Sensitive Personal Data: means personal data consisting of information revealing racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership in political parties, trade unions, organizations and associations with a religious, philosophical, political or trade-union, biometric or genetic data, or provide information as to the health or sexual life of an individual, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings and financial, or any other personal data as the Commission may determine by order published in the official Gazette.	**S.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.
Consent has not been defined.	**S.2 (l) - Consent:** consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the collecting, obtaining and processing of personal data relating to him or her.
Pseudonymisation has not been defined.	**S.2 (m) - Pseudonymisation:** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Scope: Only applies to persons, company or agency who/which process, have control over or authorise the processing of any personal data relating to Pakistani citizens.	**Scope**: The Act applies to any person, company or agency who/which process, have control over or authorize the processing of any personal data if any of the data subject, controller or processor is located in Pakistan.
Chapter II - Processing of Personal Data	**Chapter II - Processing of Personal Data**

And Obligations Of The Data Controller And Data Processors **S. 8 - Security Requirements**: Only the Data Controller was made liable to take practical steps to protect the personal data in the terms mentioned under Section 8. **S. 12 - Prohibition on transfer of Personal Data:** Any kind of personal data could be transferred to any system located beyond the territories of Pakistan only if it was ensured that the country where the data is being transferred offers personal data protection equivalent to the protection provided under this Act.	**And Obligations Of The Data Controller And Data Processors** **S. 8 - Security Requirements**: Liability now falls on the Data Controller or the Data Processor to take practical steps to protect the personal data in the terms mentioned under Section 8. **S. 14 - Cross Border Transfer of Personal Data:** Critical Personal Data can only be processed in a server or data center located in Pakistan. The Federal Government has now also been cloaked with the power to exempt certain categories of personal data from the requirement of ensuring equivalent data protection on the grounds of necessity or strategic interest of the State.
Chapter III - Rights of Data Subjects **S. 24 - Rights of Foreign Data Subjects:** Foreign data subjects have all the rights that are provided in the country or territory from where the foreign data has been collected or data subject resides if those rights are consistent with the provisions of this Act, only against the Data Controller.	**Chapter III - Rights of Data Subjects** **S. 26 - Rights of Foreign Data Subjects:** The words “only against the Data Controller” have been removed and now the Foreign Data subjects have all the rights that are provided in the country or territory from where the foreign data has been collected or data subject resides if those rights are consistent with the provisions of this Act.
Chapter IV- Processing of Sensitive Personal Data **S.26 Processing of sensitive personal data:** Exceptions laid out in which case such data can be processed which includes explicit consent of the data subject, or under instruction of the law etc. The concerning provision here is 26 (iv) (a) which talks of medical purpose, the definition of which includes the head of ‘medical research’ which is vague and broad and has the potential for ambiguity.	**Chapter IV- Processing of Sensitive Personal Data** **S.28 Processing of sensitive personal data:** Whereas the wording of the section remains verbatim, the key difference is in the definition of sensitive personal data as defined in s.2 (k) of the new draft where health now includes mental and psychological health. Other new additions are access controls (username and/or password), a more comprehensive definition of financial information. Genetic data has been taken out of the new 2020 draft definition as well as the exclusion of ‘*membership in political parties, trade unions, organizations and associations*

	with a religious, philosophical, political or trade-union' and '*the commission or alleged commission by him of any offence,or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings*' which were included in the 2018 draft.
Chapter V Exemptions **29. Power to make further exemptions** Subsection 29(1) provides very wide delegated powers to the Federal Government *"to exempt the application of any provision of this Act to any data controller or class of data controller",* thus bypassing effective parliamentary scrutiny. We recommend that the Bill is amended to limit such broad powers awarded to the Federal Government, and to ensure that any deviations from the Act be subject to an open, inclusive and transparent legislative process.	**Chapter V Exemptions** **S. 31 Power to make further exemptions** The relevant section, which in this version is s. 31 remains verbatim with only one change: previously s.29 (4) stated : '*An appeal against an order passed by the Federal Government under subsection (1) shall lie to the High Court.'* This subsection has been removed in the current draft.
Chapter VI The Commission **S.30 Commission for Personal Data Protection** (1)Within six months of coming into force of this Act, the Federal Government shall establish the National Commission for Personal Data Protection (NCPDP). (2) The Commission shall be a corporate body, having perpetual succession which can sue and be sued in its own name and **shall enjoy operational and administrative autonomy**, except as specifically provided for under this Act.	**Chapter VI The Authority** **S.32 Establishment of the Authority** The previous drafts set out the creation of a Commission to oversee the law and its implementation which in this draft has been replaced by the establishment of an Authority under S.32 S.32 (2)The Authority **shall be an autonomous body under the administrative control of the Federal government** with its headquarters at Islamabad.
Chapter VII Complaint and Offences **35. Unlawful processing of personal data**	**Chapter VII Complaint and Offences** **41 Unlawful Processing of personal data**

The fine has not been defined and must be proportionate to the Act. **S.39 Complaint** This section should provide for collective redress. The information and power imbalance between individuals and those controlling their personal data is growing and collective complaints would ensure corrective action by organisations processing personal data, which would benefit all those affected. Processing fee should not be charged by the Commission (as instructed under s.39 (3)). **S.40 Judicial Recourse** Set out grounds under which the complainant may approach High Court if not satisfied with processing of complaint. We would also like to note that while the Bill empowers the Commission to impose fines, it does not grant it the power to provide compensation to complainants who have suffered harm as a result of a data breach. We urge the Ministry to empower the Commission to direct monetary compensation to be paid in proportion to the financial, technological, social and physiological loss suffered by the complainant. The section relating to **appeal** (section 38 in the previous July 2018 version of the Bill) has been removed, this means that currently no appeals process is laid down for an aggrieved person against the decision of the Commission.	The fines have been set out for unlawful processing of personal data and sensitive personal data in s. 41 (1) and (2) respectively **S. 45 Complaint** The section remains verbatim except the word 'Commission' is replaced by the word 'Authority' in every instance. **Judicial Recourse no longer included in the new draft, instead the below mentioned section 46 on Appeal has been introduced** **S. 46 Appeal** This lays out the mechanism to appeal as available to a complainant dissatisfied with the decision of the Authority
Chapter VIII Miscellaneous	**Chapter VIII Miscellaneous**

41. Power to make rules While the power to make rules under the proposed Act has been vested with the Commission, the requirement for approval by the government calls into question the independence of the Commission. We would also challenge the extensive delegated powers awarded by section 41(2) to the Federal Government to make rules. Any changes and/or evolutions in the obligations and safeguards provided in this law must be subject to an open, inclusive and transparent legislative process.	**S. 48 Power to make rules** Verbatim, except for the use of 'Authority' instead of the word 'Commission'. No changes made or recommendations accepted in this draft.

Detailed Section-by-Section Analysis of the 2020 Bill

Chapter 1 Preliminary

Short title, extent and commencement (Section 1)

The territorial scope of application is provided for in Section 1.2, and unchanged from the 2018 version of the Bill, which states the Act would "*extend to the whole of Pakistan*", does not provide sufficient clarity on the scope of the law given that certain regions that fall within the country's boundaries are considered beyond the reach of ordinary legislation legislation such as Gilgit-Balistan, ex-FATA territories and Azad Jamu and Kashmir. This must be reviewed to ensure that the applicability of the law is clear and unambiguous.

The Bill provides for delayed implementation of the law after its legal promulation. Section1.3 states that the Act "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". While the grace period is important particularly for small businesses to develop security protocols and policies to comply with the standards set by the Bill, we would recommend a progressive implementation approach to account for pressing and egregious data protection violations during the grace period determined by the Federal Government.

Definitions (Section 2)

"Public interest" has been used as standard throughout the Bill, however has not been defined. Given that the standard allows for exemptions to the protections in the Bill, it should be defined clearly so that it does not lend itself to discretionary power.
"Critical Personal Data" has not been defined, rather it is stated explicitly in the definitions section that it is "to be classified by the Authority with the approval of the Federal Government". Critical personal data has been used in Section 14.1 to implement partial data localisation. The level of discretion given to the Federal Government in this regard is too wide and makes the implementation of the subsequent Act unforeseeable.

The definition of "personal data" (Section 2(b)) is still too restrictive as it excludes anonymized, encrypted or pseudonymized data from the ambit of personal data, which falls short of the GDPR standard. We recommend that the reference to pseudonymised and encrypted data be amended and included within the definition of personal data to make clear that pseudonymized and encrypted data is personal data. The current provision conflates pseudonymized data with anonymized data despite the differing definitions. Furthermore, encryption is a security process that should be applied to data to protect its confidentiality but does not change the nature of the data itself and should not be a process used to remove it from within the scope of the Bill.

The definition of "anonymized data" (Section 2(e)) should be revised to ensure that concerns regarding reidentification of anonymized data are adequately addressed. Several anonymised techniques can fall short of protecting personal identities given the vast amount of data it can be

correlated against. Often stand-alone anonymized data can violate the right to privacy when used in new contexts and with new sets of data, resulting in possible reidentification of data.[6] We recommend that anonymized data not be considered a static category of data, rather account for processes of reidentification by not hinging its definition on the relatability to the data subject but to the possibility to identify a data subject by ensuring that the data is rendered anonymous in such a way that the data subject is not or no longer identifiable.

We welcome the inclusion of a wide range of data to be qualified as “sensitive personal data” (Section 2(k)). In addition to those listed, we would also request that the definition for ‘sensitive personal data’ include:

- sex;
- sexual orientation;
- membership of a trade union;
- philosophical and/or religion beliefs;
- the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings or any related security measure.

The definition of “consent” (Section2(L)) is a welcome addition to this version of the Bill, however it does not mention the manner of obtaining consent from those who are below the age of majority (under 18 years) or those not in capacity to give consent (legally referred to as “of unsound mind). It is important that this Bill defines the age of majority and identifies how data of minors will be collected, stored and used. Secondly, to ensure the consent is informed all ‘terms and conditions’ of service applications should be accessible and made available in local regional languages. Thirdly, the feature of reversibility should be added to the definition of consent to ensure that data subjects are informed that their consent to having their data collected, processed, stored and shared can be withdrawn at any time.

The Bill heavily relies on consent as the legal basis for processing personal data. We would like to stress that consent is not always the most appropriate legal ground for processing personal data. Consent is a core condition of data protection which allows the data subject to be in control of when their personal data is processed, and it relates to the exercise of fundamental rights of autonomy and self- determination. However, care should be taken that consent is not relied on as a means to disclaim liability for processing and it is vital that for consent to be meaningful it is accompanied by effective safeguards. Given the power imbalance that exists between data subjects and controllers, such dangers should be counter-balanced by placing a legal burden on controllers to prove that consent was obtained in a valid, freely given, voluntary, unambiguous and informed manner, each time they wish to rely on consent as a legal basis for processing. Given that consent of the data subject is the major principle guiding data

[6] “Researchers spotlight the lie of ‘anonymous’ data”, 2019, https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/.
“Estimating the success of re-identifications in incomplete datasets using generative models”, 2019, https://www.nature.com/articles/s41467-019-10933-3.

processing, the controller should demonstrate that the data subject has given consent freely and unambiguously to processing of their personal data.

Section 11, which details the records to be kept by controllers, should also include evidence for obtained consent as an additional record. This obligation should be enforceable and enforced by the Data Protection Authority envisioned under this Bill.

Scope and applicability (Section 3)

Section 3.1 states the Act applies to “any person who processes; or has control over or authorizes the processing of, any personal data provided any of the data subject, controller, or processor (either local or foreign) is located in Pakistan.” It does not define what ‘located in Pakistan’ means but section 3.3 defines “established”. It thus needs to be clarified whether these terms are meant to be interchangeable, if so “located” should be replaced with “established” and if not, “located” needs to be defined. For example, should the data subject, controller or processor have permanent residency/place of business in Pakistan, or does it apply to anyone who is temporarily in Pakistan?

Chapter II Processing of Personal Data and Obligations of Data Controller.

General requirements for personal data processing (Section 5)

Section 5.1 allows data controllers to process personal data including sensitive personal data of a data subject with their consent, followed by a list of other conditions that may be relied upon in Section 5.2. Processing of sensitive personal data is then subject to further restrictions in Section 28.

Given that the consent of the data user is the bedrock of this Bill and invoked at several points, exemptions should be narrowly worded and limited their scope. It is reiterated that the data collector should be able to demonstrate that the data subject has consented freely and unambiguously to processing of their personal data. It should also be noted that processing of any personal data involves multiple purposes, consent should be obtained for each separate purpose.

Section 5.2 (f) states that a data controller may process personal data of a data subject without his consent if it is necessary for ‘legitimate interests pursued by the data controller’. ‘Legitimate interests’ is not defined in the Bill which may give rise to abuse and reliance on this provision for self-determined business and other interests without sufficient consideration of the impact of the processing on data subjects. At the very least this provision should be accompanied by a requirement to balance such interests with the interests, rights and freedoms of data subjects, which should always take precedent. As part of this balancing exercise data controllers should be encouraged to publish such assessments. It is important to define these terms within the context of personal data protection as it has been widely interpreted within Pakistan legal

jurisprudence; however, in the context of data protection it must encompass various, and often conflicting, ideas of privacy, personal dignity, freedom of expression and right to information.

Section 5.2 (g) risks being too broad in its scope as it allows “for the exercise of any functions conferred on any person by or under any law” without defining the nature of the law and the specificity of such functions. Blanket provisions such as this risk limiting the protections for large amounts of data and risk unnecessary and disproportionate interference with privacy and data protection rights.

Notice to the data subject (Section 6)

Providing notice is a crucial component of data protection safeguards as it ensures transparency and informed consent on part of the data subject.
Section 6.1 outlines the information data subjects must be provided when their personal data is being processed. From the list provided in points a) to h) the following are missing: i) whether the data controller intends to transfer personal data to a third country and the level of protection provided, ii) the existence profiling for targeted purpose, i.e. advertising, and the significance and the envisaged consequences of such processing for the data subject, and iii) the existence of automated decision-making and, at the very least, meaningful information about the logic involved, the significance and the envisaged consequences of such processing for the data subject. Furthermore, in section 6.1(e), regarding disclosure to third parties, it should be made clear that the default should be that named third parties be disclosed and only where there is a reasonable justification for not doing so, then the classes.

Security requirement (Section 8)

A time limit should be defined for the publication of standards by the Authority under section 8.1. The security requirements outlined in the section need to be subject to baseline and minimum requirements regardless of what is practicable, the Authority should build on these base minimums.

It should be noted that many entities use pseudonymisation and encryption as a security measure to protect personal data. The Bill, however, does not include pseudonymised and encrypted data as personal data which essentially means that as soon as any personal data is protected through pseudonymisation or encryption it escapes the ambit of the Act. Hence it is necessary that apart from personal data, the Authority should also prescribe standards to protect encrypted and pseudonymised data.

It is submitted that the Authority should also prescribe standards to protect ‘additional information’ (re: Section 2(m)) since it can be used along with pseudonymised data to discover/decode any specific personal data.

Data retention requirements (Section 9)

The period of data retention is made contingent on the “fulfilment of purpose”, however the duration of the purpose and thus retention, at the very least the criteria for retention, should be known to the data subject at the outset.

The Act should make clear how the obligation provided for in section 9 interacts with provisions in other legislation which require the retention of personal data. This is particularly relevant given the 1-year retention requirement for service providers under Section 29 of the Prevention of Electronic Crimes Act 2016 which has been previously argued is disproportionate and unnecessary for the aim pursued.[7] It is important to have clarity on whether or not the sections in this Act will supersede the data privacy provisions under PECA.

Record to be Kept by Data Controller (Section 11)

As has been mentioned above, records to be kept by data controllers should also include evidence for obtained consent. This obligation should be enforceable and enforced by the data protection authority.

Transfer of Personal Data (Section 12)

The right to data portability has not been included in the Bill. In progressive data protection regimes across the globe, data portability provides the data subject with the right to receive their data in a “a structured, commonly used and machine-readable format” and request that their personal data be transmitted to another controller without any hindrance.[8]

Personal data breach notification (Section 13)

Section 13.1 obliges the data controller to notify the Authority of any personal data breach except where the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subject. However the section does not mandate any communication or notification to the data subject.

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. The Authority should provide a clear criteria laying down all of the risks mentioned above, and others deemed appropriate, involved in a data breach from which a data controller is to assess whether a data breach is likely to result in a risk to the rights and freedoms of the data subject and thus should be informed of such a breach.

---

[7] “Privacy International's Comments on the draft Prevention of Electronic Crimes Act, 2015 (Pakistan)”, April 2015, http://digitalrightsfoundation.pk/wp-content/uploads/2015/04/Prevention-of-Electronic-Crimes-Bill-2015-Legal-Analysis_0.pdf.

[8] Art. 20 GDPR: Right to data portability, GDPR, Art. 20 GDPRRight to data portability.

Moreover, Section 13 should be amended to include an obligation to inform the data subject whose data is involved in a data breach in a timely manner, this should include providing information on steps data controllers are taking to remedy the situation, what a the data controller can do for the data subject and steps data subjects can take to protect themselves.

Furthermore, in the interest of transparency and accountability, data controllers should be required to publish public security audits of their data breaches.

Cross border transfer of personal data (Section 14)

Section 14 lays down the procedure of cross-border transfer of personal data. While it requires that the recipient country should have personal data protection at least equivalent to the protection provided under this Act, it does not monitor any onwards transfer of that personal data i.e. transfer of personal data from the recipient country to any other foreign country. Hence, Section 14 should be amended and its scope be broadened to monitor and protect any onward transfer of personal data. Section 14 also does not mention who (the Authority, data controller or data processor) is to ensure that the country where the data is being transferred offers adequate personal data protection.This is important so the data subject may know which entity to hold liable in case of a breach of this provision. Additionally, will the data controllers determine the equivalence of a country's data protection regime, or will it be determined beforehand by the Authority by way of notifications or gazetted lists? Further, because pseudonymised data is not included in the definition of personal data it will be transferred to any country without ensuring any of the safeguards mentioned in the Act. This proposition is risky because such data can be made identifiable by correlating it with other relevant additional data.

Section 14.1 provides for "critical personal data" to be processed only within Pakistan. Firstly, the term "critical personal data" is not defined anywhere in the Bill and leaves it to the discretion of the Authority to classify such data with the approval of the Federal Government.

'Processing' is defined in Section 2(f) as any set of operations such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. From this definition it follows that Critical Personal Data cannot be transferred to any system located outside of Pakistan. It is important to note that data localisation per se does not protect the safety of personal data. If other jurisdictions offer an adequate level of protection, there is no justification based on safety of personal data for preventing their transfer or imposing the storage of the personal data in a particular country. Research in other jurisdictions has shown that confining data to a few physical locations can often reduce the level of security rather than enhance it, making it vulnerable to hacking and cyber crime.[9] Further, it has been noted that in other jurisdictions the

[9] "The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India," 2019, https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf.

imposition of data localisation has been introduced as a way to facilitate unlawful surveillance and limiting the capacity of individuals to protect the confidentiality of their communications.

Section 14.1 states that critical personal data shall only be processed in a server or data center located in Pakistan. It is unclear whether the word located has the same meaning as the word ‘established’ which is used in Section 3.3. If this is the case then located should be replaced with established and if not, then the word located needs to be defined.

Chapter III Rights of Data Subjects

Right of access to personal data (Section 16)

Section 16.2 notes that a data subject must make a “payment of prescribed fee” if they submit a request to access their personal data which has been processed. Individuals should bear no cost in exercising this right. Furthermore, the requirement to furnish a data request in writing can have the effect of excluding those who are not able to file a written request due to illiteracy, lack of familiarity with procedure or disability. The requirement needs to be supplemented with an obligation placed on the data controller to provide assistance to those who wish to file a request but cannot file formal complaints due to certain limitations. These limitations may also include lack of accessibility to the Authority’s offices.

The right of access should also prescribe what minimum information the data subject is entitled to alongside a copy of their data, this should include information as the purpose of processing, the categories of the data, the named recipients with whom the data has or may be shared, the period of retention, the source of the data, their rights in relation to the data, any transfers of the data to third countries and the safeguards in place, existence of profiling and the consequences, the existence of automated-decision making, and meaningful information about the logic, significance and consequences.

Circumstances where data controller may refuse to comply with data access request (Section 18)

Section 18.1(b) allows the data controller to refuse a data access request if it cannot comply with the data access request without disclosing personal data relating to another individual who can be identified from that information. Instead of refusing access to the data on this ground, where possible, steps should be taken so that the information can be disclosed without disclosing the identity of the other individuals, for example, with redaction.

Withdrawal of consent (Section 23)

In order to ensure that Section 23 on withdrawal of consent is meaningful, it should be required that consent be as easy to withdraw as it was to provide. A comparison of the two sections (section 5 and section 23), however, shows that the process of withdrawing consent involves intricacies that make it a lot more inconvenient than the procedure of obtaining consent. While the Bill does not prescribe any specific format in which a data controller is to obtain consent

from a data subject, the withdrawal of consent has to be through a written notice. Furthermore, the requirement to furnish a notice in writing can have the effect of excluding those who are not able to file a written request due to illiteracy, lack of familiarity with procedure or disability. The requirement needs to be supplemented with an obligation placed on the data controller to provide assistance to those who wish to file a notice but cannot do so due to certain limitations. These limitations may also include lack of accessibility to the Authority's offices which makes the entire process even more cumbersome as filing a writing notice would often involve going physically to the Authority's designated office.

Extent of disclosure of personal data (Section 24)

Section 24 (d) allows the data controller to disclose the data of an individual if 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 disclosing of the personal data and the circumstances of such disclosure." This provision is too broad, and raises questions such as on the basis of what information would the data controller be able to make such a claim? Furthermore, the test of 'reasonable belief' is too low, rather a more objective standard needs to be applied in order to safeguard the interests of the data subject. In any case, the data controller should be able to demonstrate the reasons for this belief and it cannot be exercised arbitrarily.

Section 24 (e) allows the data controller to disclose the data of an individual if "the disclosure was justified as being in the *public interest* in circumstances as determined by the Authority." This provision is too broad. As mentioned above, the determination of 'public interest' must be defined by the Act, and the circumstances prescribed on the face of the legislation, not merely rely on guidance from the Authority.

It is submitted that whenever personal data of a data subject is disclosed under this section, a notice should be sent to the data subject stating therein clearly what information has been disclosed, the purpose and the lawful justification for the disclosure as well as the person/organisation/institution to whom it has been disclosed.

Chapter IV Processing of sensitive personal data

Processing of Sensitive Personal Data (Section 28)

Section 28.1 (b)(ix) allows for the collection of sensitive personal data "for the exercise of any functions conferred on any person by or under any written law". This provision raises questions regarding conflict of laws, especially with regards to broad laws violating international human rights norms regarding privacy. Data protection imperatives and privacy of sensitive personal data should override any provisions undermining the constitutional right to privacy and the spirit of this Act.

Section 28.1 (c) allows personal data to be used if it has been made public as a result of steps deliberately taken by the data subject. The meaning of 'public' is not defined and it is unclear

how wide the circulation should be to be termed as public, similarly with the term “deliberately” and how can such questions be verified. Even if an individual has deliberately made data public, this does not mean that they envisioned/ their data can be used by anyone for any purpose. This provision should be removed and at the very least interpreted narrowly.

Section 28.2 defines “medical purposes” as “the purposes of preventive medicine, medical diagnosis, medical research, rehabilitation and the provision of care and treatment and the management of healthcare services”. The inclusion of medical research goes beyond the necessity of immediate or necessary medical treatment. Refining this definition to either include a separate category for research or attaching the requirement of explicit consent is necessary.

Chapter V EXEMPTIONS

Repeated collection of personal data in same circumstances (Section 29)

It is unclear what the objective of this provision is in the Bill. Whilst further processing may be permitted all personal data should be collected for a determined, specific, and legitimate purpose. Any further processing must not be incompatible with the purposes specified at the outset (i.e. the point of collection). This essentially means that it is not acceptable to state obtain a data subject’s personal data for one purpose, and then use it for another purpose without notice, the option of withdrawing consent or justification.

We seek clarity on how this provision aligns with other principles and rights provided for in this Bill and in particular the principles of purpose limitation.

Exemption (Section 30)

Section 30.2(c) includes research and collection of statistics as exemptions for the requirement to obtain consent. This can have potential consequences, not unlike the creation of personal profiles for targeting through political advertisements in the Cambridge Analytica scandal. It is submitted that this provision be revised as it has the potential to be misused and even abused for profit. Furthermore, it is suggested that non-governmental organisations working for the public interest be included within research exemption provided for in this section.
Furthermore refining the language regarding investigative and legal proceedings, Section 25 (2)(a)(ii) in particular, by making it subject to judicial oversight and a reasonability test.

Power to make further exemptions (Section 31)

Section 31 gives the Federal Government wide powers to make exemptions to the Bill. The discretionary powers awarded to the Federal government in this section are too broad and vague. This section must be reviewed to ensure that the powers granted to the Federal Government do not permit it to bypass effective parliamentary scrutiny. These powers undermine the entire framework of the proposed legislation in light of the lack of accountability that the Government then owes to the lawmakers and the data subjects.

This situation is exacerbated by threats to the independence of the Data Protection Authority. These concerns are heightened given that the Authority would be under the administrative control of the Federal Government (Section 32.2) and given the discretion given to the Federal Government under section 32 to appoint the members of the Authority (Section 32.4), to amend the constitution of the Authority (Section 32.5), to nominate the Chairperson of the Authority (Section 32.6). We would further suggest that measures be included to ensure financial independence of the Authority. Given that the Authority is tasked with holding both the government and private companies accountable, it should completely separate from government control.

Chapter VI The Authority

Establishment of the Authority (Section 32)

Section 32.1 provides that the Authority will be established by the Federal Government so we note that this section must stipulate that the Data Protection Authority remains independent, in order to effectively and adequately fulfil its mission of enforcing the data protection framework. Adequate safeguards should be included to ensure that Authority is free from external influence, and refrain from actions which undermine the powers of or interfere with the duties of the Authority.

The composition of the Authority consists of members of the Government, including members from the Ministry of IT & Telecom, Ministry of Defence and Ministry of Interior (Section 32.4). This inclusion severely undermines the ability of the Authority to make decisions independently and without influence.

The administrative authority laid out in Section 32.12 rests with the Chairperson, however they are still “pursuant to section 38” which preserves the powers of the Federal Government to make Policy Directives. This severely undermines the independence of the Authority (see analysis of Section 38).

Powers of the Authority (Section 34)

Section 34 outlines the powers of the Authority. Section 34(2)(i) enables the Authority to prescribe a schedule of costs and mode of payment for filing of a complaint. There should be no such payment, it should be free to lodge a complaint. We do not consider that a complaint should be in a prescribed format and if so, at the very least the Authority must provide support for filing in such a format.

Furthermore, Section 34 is not explicit enough as to the sanctions available to the Authority, which should include prohibiting infringing processing as well as the power to issue substantial monetary penalties.

Power of the Authority to call for information (Section 36)

Section 36 should empower the Authority to call for information with a specified timescale.

Powers of the Federal Government to issue policy directives (Section 38)

Section 38 awards extremely broad and vague discretionary powers to the Federal government in this section. This section risks undermining the Authority's independence and autonomy. We strongly recommend that this section be removed in its entirety from the Act.

Appointment of Employees (Section 39)

Given that the Authority will be dealing with personal and sensitive personal data in the course of its proceedings, all employees and members of the Authority should be subject to a strict Code of Conduct and Data Security protocols to ensure there are no data leaks or compromise of data subjects in the course of operations.

Co-operation with International organizations (mislabelled: Section 39)

The Authority should not require prior approval of the Federal Government to co-operate with foreign and international data protection bodies, as currently provided for in section 39. Such a requirement again undermines the independence of the Authority.

Chapter VII Complaint and offences

Unlawful processing of personal data (Section 41)

Section 41 sets out the fine imposed in case of violation of the law, this should be different from the fines imposed on big data controllers/processors as defined under s.34 (d) as even the maximum cap of twenty five million may not act as a deterrent for bigger private, multinational companies in terms of financial loss.

Complaint (Section 45)

Section 45 provides that an aggrieved individual or a relevant person may file a complaint with the Authority. "Relevant person" should be defined within the Act and should include qualified representatives and certain qualified bodies, such as non-profit groups working in the field of human rights and/or data protection, to make complaints and seek remedies. The information and power imbalance between individuals and those controlling their personal data is growing and collective complaints would ensure corrective action by organisations processing personal data, which would benefit all those affected.

Section 45.3 sets out that the Authority may charge a "reasonable fee" for submitting a complaint, this should be waived in order to not bar accessibility to forums of redressal for complainants limited by affordability. Section 34(2)(i) should also be amended accordingly to remove reference to schedule of costs and mode of payment for filing complaints and its format.

We would also like to note that while the Bill empowers the Authority to impose sanctions, it does not grant it the power to provide compensation to complainants who have suffered harm

as a result of a data breach. We urge the Ministry to empower the Authority to direct monetary compensation to be paid in proportion to the financial, technological, social and physiological loss suffered by the complainant.

Chapter VIII Miscellaneous

Power to make rules (Section 48)

Section 48 notes that the Authority must have the approval of the Federal Government to make rules to carry the purposes of this Act. This requirement to seek approval from the Federal Government undermines the independence and autonomy of the Authority to effectively undertake its functions and exercise their power.

Removal of Difficulties (Section 50)

As it reads currently, Section 50 seems to permit that if compliance is too difficult to implement the Federal Government could decide to amend the law. While a standard clause in most legislation, given the unique context of data protection, this can be open to abuse and wide interpretation; particularly it holds the potential to be used by powerful data controllers to lobby removing provisions that impose costs on them, such as compliance with security requirements. Any changes and/or evolutions in the obligations and safeguards provided in this law must be subject to an open, inclusive and transparent legislative process.

Conclusion

In this detailed analysis, we have laid out both the overarching and specific concerns that we as a civil society and digital rights organisation have with the 2020 Personal Data Protection Bill. Given the nature of the subject matter of data protection and privacy in the digital age, we believe that is sustained, in-depth and multidisciplinary engagement with groups such as civil society will be needed in order to co-create a law that protects the rights of data subjects and upholds the spirit of Article 14 of the Constitution. Given the difficulties presented by the COVID-19 outbreak, we hope that the Ministry is both cognizant of these challenges and flexible in its approach. We hope for a transparent and inclusive consultation process.