PERSONAL DATA PROTECTION BILL 2021

Civil Society Submission to the Ministry of Information Technology and Telecommunications

Sep 16, 2021

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.

Contact: www.digitalrightsfoundation.pk

Concerns regarding consultation process

The Personal Data Protection Bill 2021 which has been released by the Ministry of Information Technology and Telecommunications (MOIT) is the fourth draft of the Bill released since 2018. While it is extremely encouraging that the Ministry continues to make its drafts public and open to feedback, and that some recommendations such as defining terms such as "consent" (section 2(c)) has been incorporated as well as the inclusion of section 28 which establishes data portability and right not to be subject to decisions solely based on automated decision-making. However, we would iterate that in order for a consultation process to be open, inclusive and transparent we urge that the following measures need to be taken:

1. Transparency: Currently the consultation process suffers from a lack of transparency where there is no timeline or public list of individuals and organizations consulted. Furthermore, there should be transparency regarding the kinds of objections being raised from stakeholders and a record of which recommendations have been incorporated and which have not. Reasons should be given for rejecting recommendations so that the legislative intent of the government is clear and on the record.
2. Inclusion: There is an obligation on the state to consult a diverse set of stakeholders when drafting and finalizing the law. Stakeholders should include civil society, industry representatives, the legal fraternity, academics, and individuals across the political spectrum. Including a wide cross-section of stakeholders will ensure that all aspects of data protection are captured in the Bill and result in ownership over it when it is implemented.
3. Adherence to human rights standards: Lastly, while the process itself is important and crucial, the substance of the Bill must adhere to human rights standards to ensure that Bill not only complies with international norms but also Article 14 of the Constitution of Pakistan, 1973 which guarantees the right to privacy of all persons.

Key Objections to the Bill

Digital Rights Foundation (henceforth "DRF") has submitted comments on the past three versions of the Personal Data Protection Bill (henceforth "PDPB")[1] and will continue to do so to ensure that the Bill is compliant with digital and human rights standards. While we appreciate the continued efforts to solicit comments from stakeholders on the PDPB, it has become apparent that some overarching and structural issues with the Bill have persisted since 2018 and require overhauling to comply with global standards of data protection laws and privacy rights.

Firstly, the broad powers of the Federal Government to make exemptions to the Bill (as per section 51 which grants the government unfettered powers to make rules, and section 37 giving powers of the federal government to issue policy directives) is worrisome. The large component of the data protection regime rests on holding the government--which is the biggest repository of personal data of citizens--accountable. Powers couched in broad language will give the government a freehand in interpreting the law in their self-interest and providing caveats allowing state functionaries to evade regulation.

Secondly, while it is encouraging that the Personal Data Protection Authority (PDPA) is now a commission in the form of the National Commission for Personal Data Protection (henceforth "NCPDP"), there are still concerns about the independence of the body. Firstly, as per section 32.2 the NCPDP is still under the administrative control of the Federal Government and thus does not exercise adequate independence from the executive branch. The Commission fails to meet the standards laid down in the *Paris Principles* ("Principles Relating to the Status of National Human Rights Institutions") adopted by the by UN General Assembly resolution 48/134[2] of 20 December 1993, which state that appointments to the Commission be through an established procedure, whereas in section 32.4 all appointments will be by the Federal Government and the criteria has been left up to their discretion. The Federal Government also has powers under 32.5 to "increase the number of members of the Commission and prescribe their qualifications and mode of appointment". This seriously undermines the independence of the Commission. Furthermore the power of the Federal Government to issue policy directives under section 37 undercuts the autonomy of the Commission. There must be adequate safeguards and procedures in place to make sure the Commission is independent and autonomous of the government.

Thirdly, section 14.2 states that "critical personal data" be processed inside Pakistani servers is untenable and amounts to data localization in another name. Discussions on the subject of data

[1] 2020: https://digitalrightsfoundation.pk/wp-content/uploads/2020/05/PDPB-2020_-Final-Analysis_05.05.2020-1.pdf.
2018: https://digitalrightsfoundation.pk/wp-content/uploads/2018/08/DP-Comments-Brief-Final-8.8.18-1.pdf.
[2] https://www.ohchr.org/en/professionalinterest/pages/statusofnationalinstitutions.aspx.

localization with reference to the *Rules for Removal and Blocking of unlawful Online Content (Procedure, Oversight, and Safeguards) Rules, 2020* have also proved unsustainable. We would urge the government to rethink such a proposal in the complete absence of infrastructure to support hosting and/or securing data on such a scale. In the internet age where data flows and servers operate at a global scale it would be a regressive move to practice "data nationalism". The implications of such onerous obligations would be wide-ranging as many start-ups in Pakistan rely on data servers in other jurisdictions, i.e. AWS, to operate their businesses. Data localization will also severely impact investment in Pakistan as companies might feel that the cost of shifting servers to the country is not worth the trouble.

Additionally, the new draft introduces terms such as "national interest" (section 8.1) and "national security" (section 15.2) without defining them. While public interest has been defined in the Bill, it is curious what ways in which national interest differs and why it has been left undefined. Even terms such as "legitimate interest", included in definitions (section 2(a)), fail to attach a specific meaning. Use of such broad language gives the government a wide berth to implement the law as it deems fit. Furthermore, while the right to data portability has been included in section 28.1 it is not defined; given the technical nature of these terms it is important they are adequately defined and elaborated upon. We strongly urge the Ministry to use narrow language and specific standards to ensure that the law is interpreted and implemented according to legislative intent.

Lastly, the Bill fails to account for emerging technologies and data processing techniques by way of automated decision-making and artificial intelligence. It is encouraging that the newly-added section 28 includes the "right not to be subject to a decision based solely on automated processing, including profiling" using the language of Article 22 of the *General Data Protection Regulation (GDPR)*, however the section requires further elaboration. In our previous submissions we have pointed out that the right to notice (section 6) should include adequate notice to the data subject regarding the existence of automated decision-making being applied to their data. Furthermore, a non-discrimination provision should be added as per Article 25 of the Constitution to ensure use of personal data to make automated decisions, even with a human-in-the-loop, does not result in discrimination.

Comparison between the Personal Data Protection Bill 2018 (October) and the 2021 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 2021 version:

Recommendations in Policy Brief by Privacy International and Digital Rights Foundation on 2018 PDPB	**PDPB 2020 (V.09.04.2020)**	**PDPB 2021 (V.25.08.2021)**	**Comments**
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 (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. **Anonymized Data** has not been defined	**Chapter 1 - Preliminary** **S.2 (c) - Data Controller:** a 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 (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. **S.2 (e) - Anonymized Data:** means information	**Chapter 1 - Preliminary**	

	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	**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	**S.2 (t) "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, computerized national identity card, passports, biometric data, and physical, behavioral, psychological, and mental health conditions, medical records, and any detail	

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.	detail pertaining to an individual's ethnicity, religious beliefs, or any other information for the purposes of this Act and rules made thereunder.	pertaining to an individual's ethnicity, religious beliefs, political affiliation, physical identifiable location, travelling details, pictorial or graphical still and motion forms, IP address and online identifier;	
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.		The draft lacks the mode of obtaining consent and it is necessary that such was addressed.
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		

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	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:** 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.	**Scope:** The Act applies to any person/government, controller or processor digitally or non-digitally operational in Pakistan, controller/processor even if not established in Pakistan but have control over or authorize the processing of any personal data or any other data subject present in Pakistan.	The repeated recommendation of addressing extra-territorial areas within the jurisdiction of this Act has not been implemented.
<u>Chapter II - Processing of Personal DataAnd Obligations Of The Data Controller And Data Processors</u> **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	**<u>Chapter II - Processing of Personal DataAnd Obligations Of The Data Controller And Data Processors</u>** **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	**<u>Chapter II - Processing of Personal DataAnd Obligations Of The Data Controller And Data Processors</u>** **S. 14 - Cross Border Transfer of Personal Data:** If personal data is required to be transferred to any system	

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.	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.	located beyond territories of Pakistan that is not under direct control of government of Pakistan or **entity/entities of Pakistan**, it shall be ensured that the country where the data is being transferred offers personal data protection legal regime at least equivalent to the protection provided under this Act	
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 III - Rights of Data Subjects** **S. 28 - General protected Rights:** Not contrary to any other law, the following rights of the data subject are protected under the Act. a. Right to Data Portability b. Right not to be subject to a decision based solely on automated processing, including profiling	The scope of data portability and the right to be subjected to automated processing has not been analyzed or explored fully.
Chapter IV- Processing of Sensitive Personal Data	**Chapter IV- Processing of Sensitive Personal**	**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.	**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.	**S.28 Processing of sensitive personal data:** Wording of the section remains verbatim.	
Chapter V Exemptions	**Chapter V Exemptions**	**Chapter V Exemptions**	

	S.30 Exemption Personal data may be processed for journalistic, literary or artistic purposes, provided that- f iii) the processing of personal data in the interests of the security of the State provided that the processing of personal data shall not be permitted unless it is authorized pursuant to an **express authorization by the Federal Government and in accordance with the procedure to be laid down by the Federal Government in this regard.**	**S.31 Exemption** Personal data may be processed for journalistic, literary or artistic purposes, provided that- f iii) the processing of personal data in the interests of the security of the State provided that the processing of personal data shall not be permitted unless it is **authorized pursuant to an express authorization by the Commission.**	
S.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.	**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.	**Power to make further exemptions** has been eliminated from this 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 draft 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.	**ChapterVI The Commission** **S.32 Establishment of the Commission** The previous draft set out the creation of an Authority to oversee the law and its implementation which in this draft has been replaced by the establishment of a Commission under S.32. **S.32 (2)** The Commission shall be an autonomous body under the administrative control of the Federal government with its headquarters at Islamabad.	Despite the autonomous construction of the Commission, it continues to face several restrictions. It continues to be restricted by the administrative control of the Federal government.
Chapter VII Complaint and Offences **35. 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	**Chapter VII Complaint and Offences** **S.41 Unlawful Processing of personal data** 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.	**Chapter VII Complaint and Offences**	

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 the 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	**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.		

of the Commission.			
Chapter VIII Miscellaneous **S.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	**Chapter VIII Miscellaneous** **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.	**ChapterVIII Miscellaneous** **S. 51 Power to make rules** Verbatim, except for the use of 'Commission' instead of the word 'Authority'. No changes made or recommendations accepted in this draft.	Despite making repetitive recommendations, the Commission continues to seek approval of the Federal Government to make rules and to carry the purposes. This not only makes the Commission ineffective but also defeats the purpose of creating the body in the first place.

Section-by-Section Analysis of the 2021 Bill

Chapter 1 Preliminary

SECTION 1 SHORT TITLE, EXTENT AND COMMENCEMENT

As per section 1.3 of the 2021 Bill, it is submitted that the Act shall come into force "*not falling beyond two years from the date of its promulgation*". However, it is advised that this law is brought into force with immediate effect on its promulgation as the matter of personal data and its protection requires serious consideration. While it is understandable that some data controllers

might need time to comply with the new law, however a blanket two year period is ill-advised without details of what a phased approach during that time period.

Secondly, our comment on the territorial scope of application which is provided for in Section 1.2 remains the same 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.

SECTION 2 DEFINITIONS

- The definition of "government" as per section 2 (i) restricts the scope of what can be interpreted as *government* within this Act. It is advised that this limited scope be widened to include attached departments of the government or other public bodies that might escape liability for not providing due protection to the personal data of the data subjects.
- The definition of 'legitimate interest' appears to allow data controllers to process data for any interest not expressly prohibited under the law, which is extremely wide and does not set a meaningful standard. For instance, if processing data for marketing purposes is not prohibited by law it would lead to processing without limitations. Legitimate interests should be a narrow concept involving legitimate purpose for the data controller, there should be a necessity for processing for that legal purpose while at the same time a balance should be struck between the rights of the data subject and the purpose of the data controller.

  Article 6(f) of the EU's General Data Protection Regulation (GDPR) covers legitimate interest, where it makes it subject to be overridden by 'the interests or fundamental rights and freedoms of the data subject' a caveat that is missing from the draft Bill in question. The inherent purpose of this proposed law is the protection of the rights of data subjects in Pakistan, the use of 'legitimate interests' as is, would defy that purpose. We propose that the definition be altered to include the same exception of the protection of data subjects as Article 6.

- We welcome the inclusion of a wide range of data to be qualified as "sensitive personal data" (Section 2(t)). 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 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;

-inclusion of minors' data in the definition of sensitive personal data as all data belonging to persons under 18 years of age is sensitive and demands a higher standard of protection;

- 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 Commission should also prescribe standards to protect encrypted and pseudonymised data. It is submitted that the Commission should also prescribe standards to protect 'additional information' (re: Section 2(n)) since it can be used along with pseudonymised data to discover/decode any specific personal data.

SECTION 3 SCOPE AND APPLICABILITY

Firstly, 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.

Secondly, the section needs to use clearer language to clarify that the term "government" includes governmental institutions, including but not limited to attached/ancillary departments, other public bodies such as the various bureaucratic institutions, so they are clearly brought under the scope of this law. This widened scope of the law will provide for the necessary protection of the personal data that is also the very spirit of this law.

Additionally, s.3 (1)(d) addresses 'any data subject present in Pakistan' which prompts the question of what happens when the data subject is no longer within the country's boundaries? How does the draft law plan on affording protection to the data subject in that instance?

Lastly, this section creates two categories:

1) data controllers who are established within Pakistan

2) data controllers who are operational in Pakistan but are established outside of the country.

How is the Act going to ensure the enforceability of the law on data controllers not established within the country and not subject to local laws?

Secondly, is there any mechanism to ensure that foreign data subjects whose data is held by data processors can exercise their rights in an accessible manner? Also, does section 26 mean that data controllers will have to conform to standards of data protection depending on where the subject is? If that is true then it will lead to discriminatory treatment within the category of the foreign data subject and between Pakistani-based data subjects and foreign ones.

SECTION 4 PROTECTION OF PERSONAL DATA

S. 4(2) states 'The data be collected for specified, explicit and legitimate purposes...'. Are we to assume that legitimate purpose and legitimate interest (as defined in section 2(j)) are one and the same thing? There is inconsistent language being used within the draft that adds to the confusion in understanding its ambit fully.

CHAPTER II

Processing of Personal Data and Obligations of the Data controller and Data Processors

SECTION 5 GENERAL REQUIREMENTS FOR PERSONAL DATA COLLECTION AND PROCESSING

Section 5.1 puts forward an obligation on the data controller to obtain consent from the data subject while collecting or processing the personal data. However, this section fails to point out the *mode of obtaining due consent.* It is appreciated that the law requires the data subject to give their approval each time their personal data is being processed; however, the silence on the matter makes the entire motive of the law redundant. It is advised that the data controller must not proceed before attaining the express approval of the data subject and should only proceed once they acquire the due consent.

In connection to the above, the ambits laid out in s.5 (2) (e) 'for legitimate interest pursued by data controller' and 5 (2)(f) 'for the exercise of any functions conferred on any person by or under any law.' The parameter set out is too wide for the effective protection of data subjects' interest to be maintained. We recommend that s.5 (2)(e) be removed unless legitimate interest is more clearly

defined and made subject to fundamental rights and similarly, s.5 (2)(f) also be removed since it leaves a wide berth for overriding the base principles of data protection as set out in this draft.

SECTION 6 NOTICE TO THE DATA SUBJECT

Section 6.2 requires the data controller to notify the data subject as instructed in section 6.1 within a *"reasonably possible*" time frame. This ambiguity allows the controller to abuse their position of power, and they may frustrate the reasonable period and thereby manipulate the loophole within the law to their advantage. Therefore, it will be appropriate for the legislators to introduce a time stipulation and that notices be issued in writing before any personal data is used or processed.

Also, the section does not cater to the instance where the data controllers do not serve the notice(s) despite the stipulation. It is suggested that another sub-clause, preferably section 6.4 may be added, which furnishes a penalty for non-compliance of section 6. The data controller who proceeds with personal data without serving due notice to the data subject must at least be answerable to the Commission for their non-conformity with the directions.

We would also reiterate that our comments regarding the previous draft that in the list contained in section 6.1 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.

Additionally for s.6 subsections (a), (b) and (c) should apply in conjunction, as opposed to being alternatives to one another, so the use of 'or' to demarcate the subsections should be removed and 'and' should remain instead.

As for s.6 (3), while we welcome the addition of languages being accommodated, we would like to voice our concern for those people who are not literate or are persons with disabilities.We urge that measures be taken to make the notice accessible - for instance providing the option to have the notice read through them through an audio feature etc. for it to be a fully-inclusive method of notifying all data subjects.

SECTION 8 SECURITY REQUIREMENTS

‘Keeping in mind national interest’ is a new condition for security requirements in section 8.1 in terms of the Commission’s responsibility to protect personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. Prescription of ‘national interest’ is a wide, ambiguous and subjective criteria that has the potential for misuse, as has been evident from previous legislation that has included the same condition.

The introduction of national interest when defining standards for data security could mean the privileging of state interests over that of citizens, which has resulted in future banning of encryption usage by data subjects in other jurisdictions.

Furthermore, best international standards is too vague a standard to be using in a data protection law and accords unlimited discretion to the Commission. Art 25 of the GDPR requires privacy and security by design. Other articles refer to “data minimization”. Furthermore, clear guidelines regarding minimizing access of individuals within data controller and processing organisations should be mandated as most data lapses are due to human intervention and bad faith actors. Particular to Pakistan, there are multiple instances of personal data being accessed by employees of organisations such as NADRA and telecommunication companies to weaponize that information to harass, exhort and blackmail citizens, particularly women and gender minorities. It also gives the Commission the powers of certification (Art 42), albeit voluntary. Will organizations above a certain threshold be required to conduct privacy audits? In conclusion, not providing details of what “best international standards” will look like dilutes the purpose of the section.

S. 8(4) states that ‘The data processor is independently liable to take steps to ensure compliance with security standards prescribed under sub-section (1).’ The security measures taken by the data controller should be made public and accessible to the data subject so that they can make an informed decision about whether to give the data controller access.

Lastly, section 8.5 allows for other present and future laws to become exceptions to these provisions, rendering the purpose of the section redundant. This is particularly important at a time when the Federal Government has passed a National Cyber Security Policy 2021 which will possibly set up parallel means of security compliance.

SECTION 9 DATA RETENTION REQUIREMENTS

As noted in our previous policy brief around the 2020 version of the PDPB, 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 provision for providing this information to the data subject should allow that the information be provided as per section 6(1)(b).

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 32 of the Prevention of Electronic Crimes Act (PECA) 2016 which has been previously argued is disproportionate and unnecessary for the aim pursued. It is important to have clarity on whether or not the sections 7 in this Act will supersede the data privacy provisions under PECA.

SECTION 10 DATA INTEGRITY AND ACCESS TO DATA

It is encouraging that the right to rectification and positive obligation on the data controller to ensure accuracy of data is provided under this section, a clear mechanism needs to be laid down to ensure data integrity under 10.1 and processes for data subjects to be able to rectify their data.

SECTION 11 RECORD TO BE KEPT BY DATA CONTROLLER

Section 11.3 should expand the data controller's data processing record to include categories of data, lawful basis, purpose, sharing with third parties, retention and security measures.

SECTION 12 TRANSFER OF PERSONAL DATA

Section 12 covers transfer of personal data and refers to unauthorized persons, which is not a defined term. The section should replace the term 'unauthorized person' with 'third party' or define 'authorized' and 'unauthorized' persons under the purview of the Bill. Additionally we recommend that this section either should be added to section 6, or that it be altered to mention here that even when data is transferred to a third party, due and adequate notice must be given to the data subject.

SECTION 13 PERSONAL DATA BREACH NOTIFICATION

The requirement under section 13.1 notify of breach should be the default position. The caveat that a delay can be justified when the breach is "unlikely to result in a risk to the rights and freedoms of data subject" gives undue discretion to the data controller or processor to determine what is a likely or unlikely harm; the criteria is too vague. Furthermore, it is understandable that data controllers or processors might need time to investigate the breach, it's cause and nature, however that should not preclude immediate notification to the data subject. An additional obligation can be imposed to provide detailed notification after an appropriate period of time, however a notification regarding the fact of the breach should be communicated within the 72 hour limit prescribed under section 13.1.

SECTION 14 CROSS BORDER TRANSFER OF PERSONAL DATA

As noted in the policy brief presented by DRF regarding the 2020 PDPB, while section 14 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 onward 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 Commission, 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 Commision 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.

We recommend that section 14.2 be removed from the draft as it requires data localisation. We have articulated our objection to data localisation as a practice in our previous submissions:

"'Processing' is defined in Section 2(m) 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. Further, it has been noted that in other jurisdictions the 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 15 FRAMEWORK ON CONDITIONS FOR CROSS-BORDER TRANSFER OF PERSONAL DATA

The concerns in this section are the same as those highlighted around the vagueness and width of the term 'national security' which has been added for the first time in the 2021 draft and was not a part of the data protection legislation language before. The lack of definition and the possible abuse that it may bring about in the reading of the law remains to be our prime source of concern

here and should be rephrased to be more comprehensive and definitive in its impact on the overall protection of the data subject's rights.

SECTION 16 RIGHT OF ACCESS TO PERSONAL DATA

Section 16.1 entitles a data subject to be informed when their data is being processed, however what data they will obtain exactly, is still unclear.

Section 16.2 prescribes 'a reasonable fee'. We contend that no fee should be assigned for this purpose as it can create barriers for less advantaged groups, unless the Commission wishes to add a fee for repeated or vexatious requests which carry real administrative costs.

SECTION 18 CIRCUMSTANCES WHERE DATA CONTROLLER MAY REFUSE TO COMPLY WITH DATA ACCESS REQUEST

As noted in our previous policy brief regarding the 2020 draft of the PDPB, 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.

SECTION 23 WITHDRAWAL OF CONSENT TO PROCESS PERSONAL DATA

We contend that s. 23.1 be replaced to read as 'A data subject, <u>who has consented to be a data subject</u>, may by notice in writing withdraw his consent to the processing of personal data in respect of which he is the data subject at any point in time.'

SECTION 24 EXTENT OF DISCLOSURE OF PERSONAL DATA

As contended in our policy brief on the 2020 draft and given sections 24 (d) and (e) remain the same:

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 III

RIGHTS OF DATA SUBJECTS

25 RIGHT TO PREVENT PROCESSING LIKELY TO CAUSE DAMAGE OR DISTRESS

Section 25 allows the data subject to object to their data being processed or collected for the reasons that such an act has caused them *"substantial damage or substantial distress"*, as specified in section 25.1 (b). This privilege of preventing the collection or processing of personal data comes with a few shortcomings. Firstly, the onus of proving unwarranted distress is upon the data subject, and secondly, this privilege does not seem to be given as a matter of right. Instead, it appears as a matter of discretion at the hands of the data controllers. It will be for the data subject to establish distress, and this plea of distress, having no objective standard, will be decided at the whims of the data controller.

It may be noted that section 25.3 instructs the data controller to write back to the data subject on receiving a notice from them. The data controller shall state their reasons for either compliance or non-compliance with the request. In this course, they are allowed to dismiss the request of the data subject for believing that the submitted request was either completely unjustified "*or to any extent unjustified*" as specified in section 25.3 (1)(b). Once again, there is no objective standard to gauge the *extent* of the request's rightness or wrongness, which means that the data controller will act on his subjective understanding of distress and damage.

26. RIGHTS OF FOREIGN DATA SUBJECTS

Section 26 allows for protecting personal data rights of the foreign data subjects. However, what this section fails to clarify is the question of jurisdiction of the applicable laws and the protection

that they provide their subjects with. One may question the applicability of this section: can a foreign data subject even if situated in Pakistan claim the degree of protection as promised in international regulations or vice versa? The question of territoriality and jurisdictions needs to be explained in more detail in this section with reference to a viable enforcement mechanism that can ensure any extra-jurisdictional and/or extraterritorial application

27 RIGHTS TO ERASURE

This section allows the data subject to demand for immediate removal of his personal data that has been processed illegally without his express consent. The data controller is directed to act within 14 days and ensure the erasure of such data. However, it is to be noted that the stipulation of 14 days is too relaxed a time frame when the matter is related to a person's identifiable data. This undue delay in erasing the data deprives the data subject of his right ensured within the Act. Therefore, it is suggested that this time frame is reduced to the earliest possible time and 10 days at maximum.

28 GENERAL PROTECTED RIGHTS

The introduction of the Right to Data Portability and the freedom to not be subjected to profiling and automated decisions is highly appreciated and welcomed. However, what section 28 lacks is the detail and comprehensiveness of its commitment. The right to data portability should have discussed the freedom and its limitations, if any, that allows the individuals to request the transmission of their personal data in a universally machine-readable format.

Similarly, the freedom to not be subjected to automated processing, including profiling, as set out in s.28 (b) is simply listed as such, with no parameters entailed. The right, when discussed in Article 22 of the GDPR explains the ambit, exceptions and protections necessary to be read in accordance with this right. We recommend that these two rights be set out in detail.

CHAPTER IV

PROCESSING OF SENSITIVE PERSONAL DATA

29 PROCESSING OF SENSITIVE PERSONAL DATA

Section 29 allows for data controllers to process personal data, subject to a few limitations. In the same realm, as per section 29.1 (c), the data controllers have been allowed to process personal information if the data subject had given *deliberate* permission to use the personal data on a *public* forum. As objected before, the meaning of the word ‘public’ remains undefined, and it is unclear how wide the circulation of this term can be. Even if an individual has deliberately made data public, this does not mean that they envisioned the public at large, if the case may be, to use their

data for any purpose. This provision should be removed or, at the very least, reworded to be interpreted narrowly.

CHAPTER V

EXEMPTIONS

30 REPEATED COLLECTION OF PERSONAL DATA IN SAME CIRCUMSTANCES

As submitted in our previous reservations, the scope of this section is unnecessary and it is unclear what the objective of this provision is in the Bill. While further processing may be permitted, all personal data should be collected solely 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). 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.

31 EXEMPTION

Section 31.2(c) includes research and collection of statistics as exemptions for the requirement to obtain consent from the data subjects. It is submitted that this provision be revised as it has the potential to be misused and even abused for profit as was the case in political advertisements in the Cambridge Analytica scandal. Furthermore, it is suggested that non-governmental organisations working for the public interest be included within the research exemption provided for in this section.

CHAPTER VI

THE COMMISSION

32 ESTABLISHMENT OF THE COMMISSION

Section 32.2 states that the Commission will be in the administrative control of the Federal Government. This raises serious questions regarding the independence of the Commission from the government. Given that the Commission is designed to hold all data subjects, including the government accountable, independence from the executive branch of the government is imperative. The composition and establishment of the Commission reflect the fact that it will not be independent once it is functional. Permissions from the government could be a hurdle to that independence, as well.

Furthermore, there is no properly defined procedure and criteria for appointment and removal of the members of the Commission. While section 32.4 defines the composition of the Commission broadly, they are to be appointed by the Federal Government and the government holds the power to change this composition under section 32.5 increasing the number of members of the Commission and prescribing their qualifications and mode of appointment.

34 POWERS OF THE COMMISSION

Section 34 outlines the powers of the Commission. Section 34.2(h) enables the Commission 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 Commission must provide support for filing in such a format.

Furthermore, Section 34 is not explicit enough as to the sanctions available to the Commission, which should include prohibiting infringing processing as well as the power to issue substantial monetary penalties. Such a step will play an important role and act as a much needed deterrent.

37 POWERS OF THE FEDERAL GOVERNMENT TO ISSUE POLICY DIRECTIVES

If the Federal Government continues to have an overriding power over the Commission and the general data protection laws of the state, then the very purpose of this entire legislation fails. The policy directives issued by the Federal Government should instead be vetted and approved by the Commission and its members unanimously. This will not only limit the excess of power in the hands of the government but will also provide for optimal balance. This section should be removed from the Bill.

43 COOPERATION WITH INTERNATIONAL ORGANIZATIONS

The condition of obtaining approval from the government before the Commission commits with any international Organization has a prima facie limitation to it. This condition is a clear stipulation against the Commission's purportedly autonomous and independent nature, as it will have to undergo tedious governmental procedures and undue delays to get the required approvals. This requirement will undoubtedly hamper the envisioned growth and scope of the Commission.

CHAPTER VII

COMPLAINT AND OFFENCES

48 COMPLAINT

Section 48 of the Bill prescribes a reasonable fee for the complainants who wish to file a complaint before the Commission. It is suggested that the complainants should not be charged with such payment, however minute it may be.

CHAPTER VIII

MISCELLANEOUS

51 POWER TO MAKE RULES

Section 51 notes that the Commission 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 Commision to effectively undertake its functions and exercise their power.

54 REMOVAL OF DIFFICULTIES

As it reads currently, section 54 seems to permit that if compliance is too difficult to implement, the Federal Government could decide to amend the law. This section indeed plays the role of a standard clause as found in most legislation; however, given the unique context of data protection, this can be open to abuse and broad interpretation. Section 54 particularly holds the potential to be used by powerful data controllers to lobby for removal of 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.
