DigitalRightsFoundation
"KNOW YOUR RIGHTS"

Analysis: Personal Data Protection Bill 2023

Digital Rights Foundation welcomes progress on Personal Data Protection Bill, raises questions regarding data localisation requirements and independence of proposed Commission

July 18, 2023

Executive Summary

Privacy is a fundamental human right. Protecting privacy in the modern era is essential to effective and good democratic governance. This is why data protection laws exist in over 134 out of 194 countries worldwide[1] and why we, as a civil society organisation, are keen to see Pakistan's legal framework incorporate privacy protections for its citizens.

The Digital Rights Foundation (DRF) has been actively advocating for a data protection framework in Pakistan since shortly after its inception. To that end, since the Ministry of IT (MoITT) shared its first draft of the Personal Data Protection Bill in 2018, till now in 2023, DRF has shared its feedback and highlighted policy review points on every iteration of the Bill.

About:

DRF, founded in 2013, is a 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

[1] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Introduction

DRF, as with the previous iterations of the national framework on data privacy, is keen to share our assessment of the Personal Data Protection Bill (PDPB) 2023, which was shared by the Ministry of Information and Technology and Telecommunications (MoITT) in June of 2023. The Ministry has indicated that this is the last draft and not open to public comment, however, DRF feels that the draft, while extending long overdue protections regarding digital privacy in Pakistan, needs further revision to ensure compliance with international human rights standards. DRF has identified three main areas that require work before the Bill can become law: i. removal of requirements for data localisation; ii. strengthening the independence of the Commission; and iii. removal of vague definitions of exceptions, such as 'legitimate interest'.

This fifth and apparently final draft of the Bill has incorporated some welcome developments, including section 14 concerning protection and rights regarding processing personal data of minors (individuals under the age of 18). However, the section requires specificity regarding age verification and consent processes, and revision of sub-clause 6 allowing for blanket exemptions.

Cross-border transfer of data:

Section 31(2) asks for critical personal data to be processed only in a server or digital infrastructure located in Pakistan. This, as we have previously noted, is tantamount to data localization. Concerns have been raised regarding the business viability of data localisation requirements, particularly impacting small businesses which rely on cloud servers and unhindered data flows for their work. Furthermore, in the absence of infrastructure to support hosting and/or securing data on such a scale, serious concerns regarding security of data in local servers have been raised.

Allocation of powers:

As noted previously in our comments on the 2021 draft of the PDPB, some concerns regarding the autonomy of the National Commission for Personal Data Protection

(NCPDP) have remained, such as section 35(2), which requires the Commission to be under the administrative control of the Federal Government.
In the same vein, section 43 still gives the Federal Government the mandate to create policy directives, which undermines the scope of the NCPDP.
Additionally, the government itself holds the largest repository of biometric information on the citizens of Pakistan through National Database and Registration Authority (NADRA). Allowing the government to issue directives has the potential of introducing self-serving policies is antithetical to the creation of a framework that guards citizens' best interests in terms of personal data privacy.

Additionally, section 35(1) gives the Federal Government the power to decide the number of members of the Commission and prescribe their qualifications and mode of appointment, allowing them to exert control in yet another way over the Commission.

Lack of clarity:

Certain passages of the draft invite confusion, such as the definitions of 'national interest' (section 9(1): Security requirements) or 'national security' (sections 32 and 34). The draft mentions broadly defined terms such as 'legitimate interest' (section 2(u)) and 'public interest' (section 2(ff)).
Likewise, the term 'critical personal data' is still shrouded in ambiguity and has no specifications attached to it. The draft Bill relies heavily on the NCPDP to create definitions and provide coherence to the term.

In summation, the draft Bill still requires clarity in several areas, especially in the context of terms such as national or public interest. Our concerns regarding the autonomy of the NCPDP, data localisation and implementation of the draft law persist.

We have also reviewed and given feedback[2] on the 'National Artificial Intelligence Policy'[3] put forward by the MOITT for public comment and are curious to see how these varying strands of digital governance interact with one another.

History of Data Protection Bills from 2018 to 2021:

2018: DRF lauded the efforts of the Ministry to legislate on the issue however we also raised our concerns and recommended:

a) Inclusion of public bodies under the definition of data controllers/processors.
b) Defining the scope of the Act clearly to ensure that the rights of data subjects are protected regardless of where their data is processed or held.
c) Revising and expanding the definitions of vital terms such as consent and sensitive personal data.
d) Limiting the broad powers given to the Federal Government to make exemptions to the Act.

2020: DRF submitted that the new Personal Data Protection Bill, while an improvement since its 2018 iteration, still does not fully capture the data protection needs of the people in Pakistan. Some prominent concerns other than those covered previously included:

- Exemption-making and wide-ranging powers given to the Federal Government, in particular under Sections 31 and 38, risks undermining the protections afforded under the Act.
- Lack of definition of terms such as "Public Interest" and "Critical Personal Data". It was also recommended to expand the definition of "Sensitive Personal Data" to include categories such as "membership of a trade union" and "philosophical and/or religious belief".

[2] "Feedback to Ministry of IT on Draft National Artificial Intelligence Policy 2023," Digital Rights Foundation, July 10, 2023, https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Feedback-National-AI-Policy-DRF-July-2023.pdf.
[3] 'Draft National Artificial Intelligence Policy,' MOITT, May 2023, https://moitt.gov.pk/SiteImage/Misc/files/National%20AI%20Policy%20Consultation%20Draft%20V1.pdf.

- Inadequate consent standards for personal data of children and young adults below the age of majority.
- Complicated procedure for withdrawal of consent, it was recommended to ensure that it is as easy for the data subject to withdraw consent as it is to give it.

2021: The penultimate draft presented by the Ministry had come a long way from the original version in some ways, however, we noted that some overarching and structural issues with the Bill persisted since 2018 and required overhauling to comply with global standards. Our concerns, as a digital rights organisation, were:

- The broad powers granted to the Federal Government under the Act have persisted in the 2021 version too. Power to make exemptions to the Act, when vested in the hands of the very entity that hosts the largest repository of citizen data, would deter accountability
- The lack of independence of the National Commission for Personal Data Protection (NCPDP), placing the Commission under the administrative control of the Government only sought to reinforce the validity of the point directly above and undercut the efficacy of the NCPDP.
- Data localization: multiple versions of the draft insisted on processing 'critical personal data' to essentially operate within the borders of Pakistan. These provisions are understood as regressive given the scale and fluidity of data server operations globally.

Section-by-Section Analysis of the 2023 Bill

CHAPTER I PRELIMINARY

Section 1: Short title, extent and commencement

Section 1.3 of the 2023 Bill states that the subsequent Act will come into force "not falling beyond **two years** from the date of its promulgation". It is advised that the time stipulation be lessened to six months instead of twenty-four months given the urgency with which citizens require data privacy and protections.

Section 2: Definitions

The definition of '**legitimate interest**' in section 2(u) 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. Further, the concept also appears under sections 5(2) and 6(6)(g) as exceptions which widens its scope. Hence the concept of legitimate interests should be interpreted in a restricted manner to protect the rights of the data subject from blanket exceptions to the law, the current definition is antithetical to the purpose of the legislation.

Article 6(f) of the EU's General Data Protection Regulation (GDPR) 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. We propose that the definition be altered to include the same exception of the protection of data subjects as Article 6 of the GDPR.

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.

Furthermore, the term '**public interest'** is a complex and tricky concept in general, and the definition of the same under section 2(ff) adds more confusion and vagueness. Therefore, it is recommended to define the parameters of public interest clearly and precisely to avoid its abuse.

In addition, the definition of **'vital interests'** under 2(oo) should have a time limitation for *"humanitarian emergencies, in particular in situations of natural and man-made disasters, and monitoring and management of epidemics"* as these situations can be used as a pretext to misuse, collect and store the personal data and sensitive data.

Section 3: Scope and Applicability

Firstly, the territorial scope of application provided for in Section 1.2 remains unchanged from the 2018 version of the Bill, which states the Act would "extend to the whole of Pakistan" and 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 such as Gilgit-Baltistan, ex-FATA territories and Azad Jammu 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 regarding the term "**government**" (u/s 2(o)) which 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 personal data held with all government institutions, which is also the very spirit of this law.

Lastly, this section creates two categories:
1) data controllers who are established within Pakistan; and
2) data controllers who are operational in Pakistan but are established outside of the country.

While this distinction between the two is necessary, it is important to question the accessibility of data to foreign data subjects. 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 Pakistan-based data subjects and foreign ones.

CHAPTER II: PROCESSING OF PERSONAL DATA AND OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

Section 6: Consent for personal data processing

Section 6 puts forward an obligation on the data controller to obtain consent from the data subject while collecting or processing personal data. It is appreciated that the law puts the burden of proof of the acquired consent on the data controller. However, perusal of sub-section (5) states that revocation of consent places an obligation on the data controller to direct its data processors to stop processing such data "within a reasonable time". It should be noted that such notice by the data controller should have an immediate effect except in cases when it is not reasonably practicable and in exceptional circumstances, the controller may have to justify this delay. Provision can be made for exceptions for reasonable time standards and necessary reasons furnished by the data controller to the Commission and data subject.

In connection to the above, the ambit for **exceptions** to the consent requirement–laid out in section 6(6)(g) 'for a legitimate interest pursued by data controller' and 6(6)(h) 'for the exercise of any functions conferred on any person by or under any law'–are too wide for the effective protection of data subjects' interest.

As stated earlier, the definition of "legitimate interests" is vague, which may lead to legal interpretation issues and misuse of the law. To avoid abusing the exception of legitimate interest, it is recommended that data controllers be required to do a balancing assessment between legitimate interests and the protection of data rights, if not, then at least the criteria for exceptions need to be narrowly defined according to international human rights standards and the spirit of the law. Notwithstanding, it is also recommended that section 6(6)(g) be removed unless a legitimate interest is more clearly defined and made subject to fundamental rights. Similarly, section 6(6)(h) also be removed since it leaves a wide berth for overriding the consent of data subjects.

Section 7: Notice to the data subject

Section 7(2) requires the data controller to notify the data subject as instructed in section 7(1) within a "**reasonably possible**" time frame. This ambiguity allows the controller to

define longer timeframes manipulating the ambiguity in 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 7(4) may be added, which furnishes a penalty for non-compliance to section 7. 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 our comments from the previous draft that the list contained in section 7(1), the following are missing: i) whether the data controller intends to transfer personal data to another country and the level of protection provided there, ii) the existence of profiling for targeted purpose, i.e. advertising, and the significance and the envisaged consequences of 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. However, we appreciate the inclusion of section 7(1)(d) regarding the cross-border transfer of personal data. Furthermore, in section 7(1)(f), regarding disclosure to third parties, it should be made clear that the default should be that names of third parties be disclosed, and only where there is a reasonable justification for not doing so, the classes of third parties be disclosed.

Additionally, for section 7(2) 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 section 7(3), while we welcome the addition of languages being accommodated, further accommodation should be made for people who are not literate[4] 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 to them through an audio feature,

[4] The literacy rate of Pakistan is 62.8%, meaning that millions of Pakistanis continue to be illiterate. This information may be accessed at: //www.finance.gov.pk/survey/chapters_23/10_Education.pdf

or visual-based aids that accommodate both low-level literacy and hearing impairments for it to be a fully-inclusive method of notifying all data subjects.

Section 9: Security Requirements

Prescription of 'national interest' is a wide, ambiguous and subjective criterion that has the potential for misuse. Also, the criteria of '**national interest**' when defining standards for data security could mean the privileging of state interests over that of citizens. The term 'best international standards' is too vague a standard to be used in a data protection law and accords unlimited discretion to the Commission. Moreover, clear guidelines should be mandated as data lapses can result in leaking of sensitive information which has the potential to cause great harm to data subjects. Particularly in Pakistan, there are multiple instances[5] of personal data being accessed by employees of organizations such as NADRA and telecommunication companies to weaponize that information to harass, exhort and blackmail citizens, particularly women and gender minorities.[6]

In conclusion, not providing details of what "**best international standards**" will look like dilutes the purpose of the section. section 9(4) which 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 9(5) allows for other present and future laws to become exceptions to these provisions, rendering the purpose of the section redundant.

Lastly, as the government develops policies such as the 'National Cyber Security Policy'[7] and Computer Emergency Response Teams (CERTs) are being instituted for data security,

---

[5] NADRA has initiated criminal proceedings against its employees for illegally accessing the Chief of Army Staff's family record. Details available at: https://www.dawn.com/news/1751183.
The private and confidential information belonging to Pakistani individuals has been compromised as a result of government officials irresponsibly sharing their access passwords to NADRA data. Details available at: https://propakistani.pk/2018/05/07/govt-officials-in-punjab-allegedly-sold-nadra-records-call-and-police-data-of-every-pakistani/

[6] Ehsaas programme officer had been arrested under the charge of raping a teenage girl. Details available at: https://www.geo.tv/latest/316683-ehsaas-programme-officer-arrested-for-allegedly-raping-minor-girl-layyah

[7] 'National Cyber Security Policy 2021,' Ministry of Information Technology and Telecommunications, https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf.

harmonisation with the data protection Act needs to be integrated into the law to ensure privacy rights are prioritised across the board.

CHAPTER III: PROCESSING CHILDREN'S PERSONAL DATA

Section 14: Processing personal data of children

Section 14 of the Bill introduces a legal framework for protecting children's data rights, and mitigating the risks associated with the potential misuse of personal information. Within this section, sub-clause 3(d) mentions that "such other factors as may be prescribed" should be taken into consideration for age verification and taking parental consent to process children's data. To ensure the effectiveness of this provision, it is recommended that the factors relating to age verification and parental consent be explicitly outlined to prevent any potential misuse of the law. Clearly defining these factors can ensure accountability and transparency in the process. Furthermore, it is important to ensure that the age verification process is not privacy-intrusive and does not lead to additional collection of information of the child or parent.

Additionally, given the unique socio-cultural dynamics in Pakistan, parental consent requirements have the potential for increased surveillance of children, particularly young women, and can translate into violence directed at them based on their online presence. It is important to recognise the unfortunate reality that, in some cases, parents might not be best placed to determine their child's safety.[8] In the absence of adequate social security mechanisms for the protection of children from familial violence, we need to tread carefully given the specific socio-cultural context of Pakistan.

[8] "Pakistan: Three arrested over 'honour killing' of teenage sisters," *AlJazeera*, May 18, 2020, https://www.aljazeera.com/news/2020/5/18/pakistan-three-arrested-over-honour-killing-of-teenage-sister. Azam Butt, "Woman stoned to death on panchayat's," *Pakistan Today*, July 10, 2013, https://archive.pakistantoday.com.pk/2013/07/10/woman-stoned-to-death-on-panchayats-orders/. "Boy guns down sister for using mobile phone," *Pakistan Today*, February 20, 2018, https://archive.pakistantoday.com.pk/2018/02/20/boy-guns-down-sister-for-using-mobile-phone/. "Gujranwala man kills sister over mobile phone," *The Nation*, October 17, 2021, https://www.nation.com.pk/17-Oct-2021/gujranwala-man-kills-sister-over-mobile-phone. "Man kills daughter in Charsadda over dance video on social media," Dawn, January 23, 2023, https://www.dawn.com/news/1733115.

Furthermore, the exception under subsection 6 is very wide, which may lead to ambiguous legal interpretation and misuse of the law. Therefore, it is important that this exception is rephrased and is limited in nature.

Additionally, the Bill needs to have clarity on the international business practice of allowing children above the age of 13 to access and use digital services. For instance, most social media platforms allow 13-year-olds to set up accounts. This might create a hindrance for digital platforms to operate in Pakistan, and thus the processes through which these protections accorded to children are enacted need to be clarified for businesses.

CHAPTER IV: ADDITIONAL REQUIREMENTS FOR PROCESSING SENSITIVE AND CRITICAL PERSONAL DATA

Section 15: Processing of sensitive and critical personal data.

Section 15 (a) (viii) lays out an exception '*for the administration of justice under the orders of a court of competent jurisdiction*' regarding the processing of sensitive and critical personal data of a data subject. We submit that this exception should be subject to the fundamental rights afforded to the citizens, i.e., data subjects in question, especially the right to privacy enshrined in Article 14 of the Constitution of Pakistan.

Section 15(b) states: "*The Commission may by order published in the Gazette exclude the application of clauses (i), (viii), or (ix) of clause (b) of sub-section (1) in such cases as may be specified in the order…*". It should be noted that clause (b) of subsection (1) does not contain any subclauses. There is a typographical error as these clauses fall under clause (a) of sub-section (1) instead and should be corrected before the draft is finalised.

CHAPTER V: RIGHTS OF DATA SUBJECTS

Section 16: Right to access

Whilst the inclusion of the right of data subjects to access the information data controllers have on them is a positive development, this right becomes inaccessible due

to 16(3), which imposes a "prescribed fee" on anticipated "administrative costs" to provide this personal information report. This imposes an unreasonable burden on the data subjects, whose ability to access their personal data should not be contingent on their ability to pay a fee. Such a service should be provided free of cost, with any and all administrative costs being incurred by the data controller.

Section 17: Compliance with data access requests

Under this section, whilst a timeframe within which the data controller has the obligation to respond to the data access request has been defined, it does not stipulate any penalties for failing to comply with such a request for reasons not furnished in Section 18 (Circumstances of refusal to comply with the data access request).

Section 18: Circumstances of refusal to comply with the data access request

It is recommended that in the event that the circumstances meet the criteria set in section 18 of the Act, the data controller must provide the data subject requesting access to their personal data with reasons for the refusal of the request in writing in the timeframe stipulated in s 17(1) and s17(3).

Section 26: Right to erasure

The stipulated time frame of 14 days is overly relaxed, particularly when dealing with a person's identifiable data, and undue delay in erasing the data deprives the data subject of their right ensured within the Act. Therefore, it is recommended that this time frame is reduced to the earliest possible time and 05 days at maximum and every subsequent day delaying the erasure should be justified with explicit reasons sent to the data subject and Commission.

Section 27: Right to nominate

This is a new addition to the draft, however, the wording of this section needs to be altered. The current version suggests that a data subject, after his death, may nominate another individual to exercise rights over his data. The section may be rephrased as follows: *"In the event of the death or disability of the data subject, any other individual as may be prescribed or previously nominated by the data subject himself, may exercise the rights of the data subject under the provisions of this Act."*

Section 28: Right to redressal of grievance

We welcome this new addition to the draft, however, it is necessary to point out that this section does not adequately elaborate upon the functionality of the redressal system in case a data subject faces any grievance. Since this is the first forum of complaint available to the data subject, the provision needs to elaborate upon it just as the complaint submitted to the Commission is expanded upon within the draft.

For instance, data controllers, as per their existing resources, could potentially chalk a redressal mechanism wherein they address complaints, in writing, within five working days of having received the complaint. In case of any delay, these controllers may be required to explicitly explain the same, once again, in writing to the aggrieved party.

Section 29: Right to data portability and automated processing

Section 29(6) raises the '**public interest**' exception to the right to data portability and automated processing. In contrast, Article 9(2)(g) of the General Data Protection Regulation (GDPR) of the European Union posits the following exception:

"g) *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".*

Article 9 broaches the subject of public interest with important parameters to strike a balance between the mandate of public protection and individual rights. Similar safeguards need to be implemented within the Bill for public interest exceptions.

Additionally, any **automated decision-making** based on personal data needs to be accompanied by robust and explicit anti-discriminatory policies, which must be communicated by data controllers to the data subjects, and grounded in Constitutional protections as per Article 25.

Section 31: Condition for Cross border transfer

Subsection 2 stipulating that '**Critical Personal Data**' only be processed in a server(s) or digital infrastructure located within the territory of Pakistan is a **data localisation**

requirement which is contrary to principles of an open internet and can undermine the security of data.

Currently, Pakistan lacks the infrastructural capacity to provide cloud storage for local and international businesses making the implementation of this requirement impossible. Furthermore, the Bill fails to consider practical requirements such as the lack of electricity and energy supply in order to run such data centers. The IEA finds that "data centres and data transmission networks are responsible for 1% of energy-related GHG emissions," which could translate into a significant environmental impact for Pakistan, and estimated global data centre electricity consumption was "240-340 TWh1, or around 1-1.3% of global final electricity demand."[9] In a context where Pakistan already does not have the resources to meet current energy requirements,[10] with local industries suffering due to load-shedding and unreliable electricity supply,[11] regular nationwide grid failures,[12] and natural disasters[13] data localisation is not a practical or economically viable option.

Data localisation requirements are particularly onerous for local small business and data controllers who often rely on cloud services, which are extraterritorial servers, and has been objected to by larger international corporations as it makes service delivery

[9] "Data Centres and Data Transmission Networks," *IEA*, https://www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks.
[10] Jawad Malik, "Pakistan's energy shortfall 'surpasses 8,500 megawatts'," *The News International*, June 25, 2023, https://www.thenews.com.pk/latest/1084421-pakistans-energy-shortfall-surpasses-8500-megawatts.
[11] Aamir Khan, "Power outages add to business community's woes," *The Express Tribune*, June 4, 2022, https://tribune.com.pk/story/2359944/power-outages-add-to-business-communitys-woes.
[12] Abid Hussain, "Pakistan hit by nationwide power outage after grid failure," *AlJazeera*, January 23, 2023, https://www.aljazeera.com/news/2023/1/23/pakistan-hit-by-nationwide-power-outage-after-grid.
"Nationwide power blackout plunges Pakistan into darkness," *The Guardian*, January 20, 2021, https://www.theguardian.com/world/2021/jan/10/pakistan-power-gradually-being-restored-after-nationwide-blackout.
[13] Surabhi Sahu, Kenneth Foo, and Haris Zamir, "Pakistan floods endanger power plants, aggravate energy crisis," *S&P Global Community Insights*, September 14, 2022, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/energy-transition/091422-pakistan-floods-endanger-power-plants-aggravate-energy-crisis.
"Massive outages hit Pakistan's north after flash floods damage over 20 power houses," *Arab News*, September 25, 2022, https://www.arabnews.pk/node/2147616/pakistan.

nearly impossible.[14] This will significantly increase the cost of doing business in Pakistan, particularly damage to the country's economy and the pro-IT policies of the government in the form of Digital Pakistan and tax concessions given to the IT sector under the current (2023-24) budget.[15]

Section 32: Framework on conditions for cross-border transfer

The new addition of sub-sections (a), (c) and (d) in the fresh draft undermine the purpose of the necessary explicit consent requirement as was introduced previously. In short, the subsections (a), (c) and (d) nullify the requirement of *explicit consent of the data subject* mentioned under section 32 (1) (b) presently, meaning that in case of an agreement/contract, the personal data may be transferred regardless of having obtained explicit consent of the data subject. The consent of a data subject should be deemed primary when deciding the transfer of data.

Further, not providing details of "any further conditions specified by the Commission" as mentioned under section 32 sub-clause 1(d) dilutes the purpose of the entire section. We recommend that the conditions that would be considered by the Commission should be made public and accessible to the data subject, allowing them to make informed decisions.

Moreover, the terms "national interest" and "public order" used in this section form a wide, ambiguous and subjective criteria that has the potential for misuse. The vagueness of this criterion accords unlimited discretion to the Commission.

Section 34: Exemption

Section 34(2)(c) includes **research** and **collection of statistics** as exemptions for the consent requirement 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

[14] In its letter addressed to then-Prime Minister Imran Khan, the Asian Internet Coalition (AIC) highlighted their concerns regarding the impact of the requirement for data localization from a business lens, citing multiple issues in section 3.3 of the Appendix.
"AIC Submits a Letter to the PM on Removal and Blocking of Unlawful Content," Asia Internet Coalition, December 2020,
https://aicasia.org/policy-advocacy/pakistan-aic-submits-a-letter-to-the-pm-on-removal-and-blocking-of-unlawful-content/.

[15] "Dar pins hope on IT sector to become engine of growth in coming years," Associated Press of Pakistan, June 9,
2023,https://www.app.com.pk/business/dar-pins-hope-on-it-sector-to-become-engine-of-growth-in-coming-years/.
Tahir Amin, "IT sector: Budget brings in huge incentives," Business Recorder, June 10, 2023,
https://www.brecorder.com/news/40247003.

the Cambridge Analytica scandal. Furthermore, it is suggested that non-governmental organizations working for the public interest be included within the research exemption provided for in this section.

Moreover, the newly inserted sub-section 4 is vague, broad, and ambiguous. The term "**specific situations/use cases**" gives undue discretion to the Commission to determine the situations or cases in which the Federal Government will be exempted. Hence the term "specific situations/use cases" should be precisely defined, or additional conditions may be imposed on the situations in which the Federal Government can be exempted.

Section 34(2)(f) lays out an exemption for **'journalistic purposes'** that curtails provisions of section 16(1) that allows data subject access to their personal data by the data controller, section 6 consent for processing, section 7 notice to data subjects, section 8 non-disclosure of personal data, amongst others. This is a wide ambit of exceptions, particularly with regard to critical personal data and sensitive personal data. We already have seen and recorded a sizable number of instances where data breaches have occurred, especially those impacting women and gender minorities. We propose that explicit requirements be set down by the NCPDP to chart out SOPs to safeguard such vital data whose exploitation is a well-documented phenomenon. Such guidelines should come into force within 6 months of the enactment of this law.

Section 35(2): Establishment of the Commission

Section 35(2) states that "*the Commission shall be an autonomous body under the administrative control of the Federal Government with its headquarters located in Islamabad*." Please note the contradiction within the section as the idea of an autonomous body implies that the Commission, without any undue influence of any external bodies; however, the latter part of the same sub-section (section 35(2)) places it under the administrative control of the Federal Government negates, which the very concept of autonomy.

In light of the above, it is recommended that the Commission should be removed from the administrative control of the Federal Government and that safeguards be included in the section to ensure its independence as per international best practices, such as the 'Principles relating to the Status of National Institutions (The Paris Principles)'.[16]

[16] UN General Assembly, "Principles relating to the Status of National Institutions (The Paris Principles)," resolution 48/134, December 20, 1993, https://www.ohchr.org/en/instruments-mechanisms/instruments/principles-relating-status-national-institutions-paris.

Section 37: Special provisions concerning members.

Previously, in the 2021 draft, under section 32(8) the term "misconduct" included 'corruption and dishonesty' but in the new draft, under section 37(2), the term is not further defined, and there is an addition of the word "misappropriation." Both the terms are wide, ambiguous, and subjective in nature, with the potential for misuse. The vagueness of these criteria accords unlimited discretion to the Commission. The lack of definitive criteria throughout the draft Bill remains our primary concern and should be rephrased or defined accordingly.

Section 43: Powers to issue policy directives

This power accorded to the Federal Government binds the Commission to policy directives and severely undermines the independence of the Commission.

Section 47: Cooperation with international organizations

The condition of obtaining approval from the government before the Commission cooperates with any international organization is a prima facie limitation. 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 IX COMPLAINT AND OFFENSES

Section 51: Complaint

The section 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 small an amount it may be.

CHAPTER X MISCELLANEOUS

Section 54: Power to make Rules; Section 59 Dissolution

The Bill lays out that the Commission shall make rules to execute the purposes of this Act with the approval of the Federal Government. However, Section 54 gives absolute power to the Federal Government to make the rules. Similarly, under section 59, the Commission can be wound up by the order of the Federal Government - contrary to the previous draft, which allocated the Parliament the power(s) of winding up the Commission. These amendments give undue power to the executive branch of the state, hence disrupting the foundational concept of separation of powers.