# Media Matters for Democracy Personal Data Protection Bill 2020

## Concerns, Comments and Recommendations


Policy Research & Advocacy Initiative

MediaMatters forDemocracy
Policy Research & Advocacy Initiative

# Personal Data Protection Bill, 2020

## Concerns, Comments and Recommendations

**About Us**

Media Matters for Democracy (MMfD) is a not-for-profit organization working to defend digital rights, freedom of expression, media, the internet, and communications in Pakistan. We focus on policy research, advocacy, training, legal aid and support, and public interest litigation.

**Contacts**

Sadaf Khan - Co-Founder, Director Programs
Media Matters for Democracy
sadaf@mediamatters.pk

**Acknowledgements**

This analysis has been written by Hija Kamran, Salwa Rana and Zoya Rehman.

We are thankful to Jannat Ali Kalyar, Umer Gilani, Yasser Latif Hamdani and Zeeshaan Zafar Hashmi for their additional input and suggestions.

## Overview

Privacy is an internationally recognized human right, enshrined in not only the Universal Declaration of Human Rights[1], but also the Constitution of Pakistan. Article 14 of the Constitution states that "the dignity of man and, subject to law, the privacy of home, shall be inviolable." Privacy and data protection are inherently linked; the protection of personal data has long been recognised as a fundamental aspect of the right to privacy. This discourse gained precedence in Pakistan after the passage of the European General Data Protection Regulation (GDPR) that outlines a holistic approach to data protection regimes for the member states of European Union, and people's right to privacy and data protections in general.

The Government of Pakistan made a commitment to introduce data protection legislation when it signed the Open Government Partnership in 2017, the status of which is now inactive given Pakistan's failure to submit action plans and subsequent updates. Two draft bills of the Personal Data Protection Regulation were shared in 2018 by the Ministry of Information Telecommunications and Technology (henceforth referred to as 'the Ministry'). Media Matters for Democracy recently published a statement in which it expressed concerns about the government's excessive use of digital surveillance technologies, and urged for a new protection law in light of the consultations with the Ministry that have been ongoing since 2017[2]. A day later, the Ministry released the draft Personal Data Protection Bill, 2020 (henceforth referred to as 'Draft Bill') on its website and invited input from relevant stakeholders.

Media Matters for Democracy has been involved in the consultative processes leading to this Draft Bill since 2017. Therefore, we welcome the call for input that has been initiated by the Ministry and take the opportunity to raise concerns regarding the Draft Bill. The current draft is problematic in that it does not guarantee key human rights protections to Pakistani citizens, and seems to give the Federal Government discretionary powers in regards to people's personal data.

We do not wish to see this law follow the footsteps of other draconian internet rights legislation initiated by our government. Therefore, as part of this consultative process, we call on the Ministry and the government of Pakistan to review the areas of concern flagged in this analysis, and provide a guarantee to the citizens of Pakistan that personal data is effectively and necessarily protected. We hope that the Ministry will consider the recommendations and concerns on the bill highlighted in this document, and aim to pass a regulation that unconditionally prioritises the protection of citizens' data and their right to privacy.

1 Article 12 of the UDHR proclaims, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence….. Everyone has the right to the protection of the law against such

2 interference or attacks."

Joint Statement to the Federal and Provincial Government(s) of Pakistan on Our Concerns Regarding the Excessive Usage of Digital Surveillance Measures and the Lack of Data Protection Laws During the Ongoing Coronavirus Pandemic

http://mediamatters.pk/joint-statement-to-the-federal-and-provincial-governments-of-pakistan-on-our-concerns-regarding-the-excessive-usage-of-digital-surveillance-measures-and-the-lack-of-data-protection-laws-during-the-o/

**Concerns Regarding the Draft Personal Data Protection Bill, 2020**

1. The Draft Bill fails to clearly define some of the most fundamental and recurrent terms in the law. The vague definitions and language, and the use of overbroad terms like "vital interests", leave exceptions for protections in regards to citizens' rights, and are left open to judicial interpretation. Terms such as "critical personal data", "legitimate interests" and "strategic interests" have not been included in the Definitions section even though they have been used frequently in the Draft Bill. Such terms create exceptions for the state in regards to national security, law enforcement and sovereignty. This drops the **legal test of 'necessity and proportionality' and legality.**

2. **Personal data itself has not been properly defined.** The interchangeable use of personal data, critical personal data (which has been left undefined) and sensitive personal data renders the classification of different forms of personal data confusing and weak.

3. No **distinction** has been made among individuals, government bodies and the private/commercial sector. This categorization is quintessential not only in terms of providing a reason as to why the data is being used by data controllers and processors, but also to shed clarity in regards to the responsibilities, liabilities, or protections that are outlined in the Draft Bill. A distinction also needs to be created among the different kinds of **government bodies** that exist in Pakistan and collect people's personal data. Moreover, the size and nature of operations must also be considered, in order to gauge the **capacity** of a person, small organization, corporation, or government body to collect and process data separately.

4. The Draft Bill should acknowledge that **anonymized, pseudonymized and encrypted data** can be personal data as well, and can be identified using basic variables[3] in a dataset.

5. We find the generic requirements to localize / mirror all sorts of data troubling. We do not support **data localization** and for copies of people's personal data to be retained in Pakistan, as we believe that this makes the personal data of Pakistani citizens more vulnerable to breaches and abuse.

6. The definition of **consent** needs to be expanded so as to make it reversible, Moreover, there should be a section that details the obtainment of informed consent, and emphasizes that consent should be taken every time someone's personal data is used for something, while also referring to specific instances such as the transfer of someone's personal data to another country. There should be stricter stipulations for consent in the case of underage

3 'Anonymised' data can never be totally anonymous, says study
https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds

Pakistanis. Moreover, the procedure for withdrawing consent should be simpler. Once the consent is withdrawn, the data processing should immediately be ceased without exceptions.

7. The Draft Bill should not give the **Federal Government excessive and exceptional powers,** nor should it encourage its increased involvement in protecting citizens' data. The government should be held equally accountable in regards to the collection and retention of people's personal data. Similarly, the Federal Government should not be allowed to consider **exemptions** in regards to data controllers without any clear procedures or measures for ensuring accountability.

8. We are particularly concerned about the **Data Protection Authority** that has been envisioned in this Draft Bill. This authority is not independent from the Federal Government, and relies on the government for not only administration but also membership and funding.

**Clause-Wise Analysis and Recommendations**

| Section | Concerns | Suggestions |
|---|---|---|
| Enactment | Due to the time period of up to two years before it comes into force, Pakistan will remain without data protection until 2022/23. The Bill also provides for delayed implementation of the law after its legal promulation. | Due to the time period of up to two years before it comes into force, Pakistan will remain without data protection until 2022/23. The Bill also provides for delayed implementation of the law after its legal promulation. |
| 2. Definitions | Some key definitions are missing from the Bill. These include "public interest", "critical personal data" and "strategic interests". We find it problematic that Critical Personal Data has not only been undefined but also been left open "to be classified by the Authority with the approval of the Federal Government." | Define "public interest" and mention "vital interests" instead of "strategic interests" for more clarity. |
| 2a. "data subject" | Without including legal persons in the definitions, it excludes the data of | The definition should include both natural and legal persons. |

| | | |
|---|---|---|
| | legal entities such as corporations and other businesses. | |
| 2b. "personal data" | The Bill presents more definitions of personal data than needed (eg. sensitive, critical). This can cause confusion in the application and the interpretation of the law by the Courts and the relevant Authorities. Moreover, this definition should not exclude anonymized, encrypted or pseudonymized data. Encrypted data, in particular, entails a security process that underscores the confidentiality of the personal data that is being shared. | The Government should consider streamlining the definitions to avoid confusion in the application of the law. This means that the addition of "critical personal data" in 2(o) should be removed and the definition of "personal" and "sensitive personal" data should be expanded to include all kinds of data.<br>In the definition of "personal data" anonymized, encrypted and pseudonymized data should be explicitly included as this data continues to be sensitive in nature and has the ability to identify the person using common, seemingly non-identifiable variables. |
| 2c. "data controller" | Extending the scope of data controllers to a natural person means that individuals could be held liable for data collection under this law. | Natural persons should be omitted to include only legal persons and government bodies. |
| 2d. "data processor" | The definition does not specify the kinds of legal persons/bodies and government bodies that will be allowed to process data. | The definition should be expanded in scope so as to include the types of legal persons and bodies, including government bodies. |
| 2g. "third party" | This definition is ambiguous, and leaves a lot of room for misuse. It needs to be clear in terms of who qualifies as a 'person', and whether it is a natural person or a legal person. The definition neither defines the | Part (v) of the section should be rephrased so as to include data controllers and data processors as defined above in Section 2(c) and 2(d). |

| | | |
|---|---|---|
| | the instances where authorization can be given in part (v), nor does it specify who the 'person' authorising it could be. These open-ended exemptions could be misused by data processors/controllers and leave room for inconsistent interpretation by Courts. | |
| 2l. "consent" | This definition does not include minors. Moreover, the reversibility of consent is not explicitly stated in this definition. | It should be stated that consent is reversible. Moreover, it should be stated that consent should be taken every time someone's personal data is used for something or by someone that they have not explicitly given consent for. |
| 2n. "vital interests" | This definition is extremely open-ended and leaves room for misuse and inconsistency in interpretation. | "Vital interests" should be clearly and more narrowly defined. |
| 2o. "Authority" and"Critical Personal Data" | A separate definition for critical personal data is unnecessary as the Bill already defines personal data and sensitive personal data. Having three different categories to divide data will cause a number of problems in the application and interpretation of the law, along with overlaps with the other definitions.<br><br>Moreover, assigning the Authority the responsibility to define "critical personal data" indicates malice on the part of the Government. This power resides with the legislature alone. The Authority, if allowed to define these terms, will be overstepping its power | It is advised that the category of "critical personal data" be omitted altogether to avoid confusion and overlap with the existing definitions of "personal" and "sensitive personal data." Moreover, if a new category has to be created, the Authority should not be given the power to define it, as that would constitute excessive delegation of legislation. |

| | | |
|---|---|---|
| | of delegated legislation and can be declared illegal by Courts. | |
| 3: Scope and Applicability | This section hinges on data localization, and entails jurisdiction over foreign entities. We do not believe that data localization guarantees the protection of people's personal data in any way. Moreover, the obligation mentioned in Section 3.2 places an unnecessary burden on companies and businesses based outside Pakistan and discourages economic activity. The GDPR also does not have a requirement of a local representative. | It is advised that the requirement of a local representative should be removed and replaced with a focal contact person within the company that is controlling the data. This person should be allowed to be based outside of Pakistan. |
| 4: Protection of Personal Data | This section does not mention "sensitive personal data". | Include "sensitive personal data" in the section. |
| 5: General Requirements | The terms "vital interests" and "legitimate interests" (f) are too broad and can lead to arbitrary decision-making. The term "legitimate interests" has not been defined in the Bill in any case. Moreover, we do not think that a data processor or controller should even be given this much discretion to interpret these terms in the first place.<br><br>An important point to highlight here is that while consent has been mentioned in this section, the exact procedure and requirements for the obtainment of consent have not been mentioned. | Both "vital interests" and "legitimate interests" must be clearly defined in the Definitions section.<br><br>There should be a separate section that specifically elucidates how consent is to be obtained from a data subject. Moreover, what qualifies as consent needs to be detailed in that section as well. That section should also note that informed consent needs to be obtained each time a data subject's personal data is collected, processed or shared. |

| | | |
|---|---|---|
| 6: Notice to the Data Subject | 6(1) does not include the instance where a data subject's personal data is being transferred to an entity outside of Pakistan, as well as the protections the data will be accorded.<br><br>In 6(1)(e), the classes of third parties are not defined. This can result in inconsistencies and be extended to any 'third party' on an ad hoc basis.<br><br>In 6(2), the phrase "as soon as reasonably possible" is vague and gives the data controller the leeway to make decisions arbitrarily.<br><br>Moreover, 6.2(c)(ii) does not factor in the consent of the data subject before the data can be disclosed to an (unknown) third party. | The Bill must clearly define the type of third party the personal data is being disclosed to. Moreover, the transfer of data to a third country, and what measures will be taken to ensure the protection of personal data in this case, should be mentioned.<br><br>It is strongly advised that "as soon as reasonably possible" be removed and replaced by a fixed and certain time-frame decided by the legislature to ensure effective implementation of the law.<br><br>Moreover, consent needs to be factored into this section. |
| 8: Security Requirements | The procedure and timeline for the Authority to prescribe "standards" have not been mentioned in 6.1. Moreover, there is no mention of SOPs for the "practical steps" that data controllers/processors need to take to protect people's personal data. | A limitation period needs to be stipulated for the standards to be shared. This section should also mention the protection of anonymized, pseudonymized and encrypted personal data. It also needs to refer to the SOPs that will be instituted for data controllers/processors to follow. |
| 10: Data Integrity & Access to Data | In 10(2), the statement "except where compliance with a request to such access or correction is refused under this Act" is vague and can be misused at the expense of the dignity of the data subject. | It is recommended that such vague statements be removed completely. The Bill must clearly stipulate exceptions in which the data subject cannot be given access to their personal data. Although it is advised that these exceptions be kept as minimum as possible to avoid infringing their rights under the law. |

| | | |
|---|---|---|
| 11: Record to be kept by Data Controller | There is no mention of how this record would be maintained. This should not be left up to the Authority. | This section should also include recorded evidence for obtained consent, which should be enforced by the independent body (in this case Authority) conceptualized under the Draft Bill. |
| 12: Transfer of Personal Data | "Unauthorized person or system" has not been defined in the Draft Bill. | Define authorized person/system. |
| 13: Personal Data Breach Notification | In 13(1), the statement "except where the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subject" is vague and can lead to misuse. It is also highly problematic to let data controllers determine what constitutes a genuine threat to the "rights and freedoms" of the data subject. It must not be left up to the data controllers to decide the kind of events in which they must notify the Authority and the data subjects since they should owe an obligation to both parties under the law.<br><br>The section also places no obligation on the data controllers to give a notification to the data subject, which also goes against the standard set by the GDPR. | We recommend that the legislature clearly defines exceptional events in which the data controller may be excused from the obligation to notify the Authority and data subjects. It is also strongly suggested that vague statements like "risk to the rights and freedoms of data subjects" should be removed altogether. If they are used to create exceptions, then they must be defined in detail by the Parliament. Data controllers data should also be obligated to disclose security audits of their data breaches for the sake of public interest. |
| 14: Cross Borde Transfer of Personal Data | This section mandates that if the personal data is being transferred to any system or server located outside of Pakistan, the data protection regime should match the one in Pakistan. It is imperative to note that no other country has a data | The requirement of data localisation should be omitted, and it should be ensured that the protection of citizens' data remains paramount. In case of non-compliance to offer the required protection, the framework |

| | | |
|---|---|---|
| | protection regime similar to Pakistan's. Moreover, it is unclear as to who is being held liable in regards to the responsibility of the country where the data is being transferred.<br><br>In Section 14(1), the lack of clarity on what constitutes "critical personal data" under this bill (see 2(o)) remains. Moreover, the requirement of "citizens' personal data" to be stored only in Pakistan could increase the risk of this information being breached. An important example of this problem is that of businesses or entities operating on the basis of a model that requires spreading out the data in order to ensure that it remains secure and/or is not lost in case one server is compromised or damaged. In addition, this requirement will directly impact the digital economy of Pakistan forcing big corporations to halt their services in the country, given the financial burden localising the servers would demand from them.<br><br>Section 14(2) has left the categories of personal data to be determined by the Federal Government, thereby making the law ambiguous and open to interpretation. Furthermore, the statement "on the grounds of necessity or strategic interests of the State" is vague and can be applied arbitrarily by the Federal Government. | should instead demand accountability in instances of data breach, and clearly mention who is being held liable in the case of personal data being transferred outside of Pakistan.<br><br>The power to exempt certain categories of personal data should be determined by the legislature. These exemptions should be clearly laid out in Section 14. Moreover, the legislature must clearly define what "necessity" and "strategic interests" means in the context of this law. |

| | | |
|---|---|---|
| 15: Framework on Conditions for Cross-Border Transfer of Personal Data | Section 16(2) mandates a fee in order for the data subject to be able to access their data in possession of a data controller. This requirement hinders the right of access for those who cannot afford to pay the said fee. Further to this, this section also puts the requirement of written complaint to access data. This is discriminatory towards those who cannot submit the request in writing either due to their lack of ability to write, or for their lack of awareness of the process. The section gives a clear indication of putting the onus of following lengthy procedures on the data subjects, instead of affirming the data controller's responsibility of respecting and ensuring the data subject's right to access. | There should not be the requirement of submission of a fee for data subjects to gain access to their own data. In addition, the requirement of written complaint should not lie entirely on the data subjects, especially when they deal with certain challenges in the process, financial, literary or otherwise. |
| 23: Withdrawal of Consent to Process Personal Data | Section 23(2) mandates the data controller to cease processing of personal data of the data subject; it does not specify the time frame for the ceasing of data processing to go in effect.<br><br>Section 23(4) stipulates a criminal liability, which would be problematic since, as suggested earlier, data controllers must not be individual (natural) persons but rather a public body/ private business / corporation. In such a situation, a civil remedy would be an appropriate alternative. | This section should clearly specify the time frame for data processors and/or controllers to halt processing of personal data upon receiving withdrawal of consent to process personal data.<br><br>It is recommended that the criminal liability attached to this section must be removed in accordance with international best practices on data protection and the GDPR. |

| | | |
|---|---|---|
| 24: Extent of Disclosure of Personal Data | The mention of "reasonable belief" in part (c) and (d) is vague and since there is no objective standard as to what constitutes a "reasonable belief", it leaves a significant amount of room for misuse and subjective interpretation that could be damaging to the implementation of the law. It also provides data controllers with ambiguous guidelines that allow them to escape liability quite easily.<br><br>Moreover, the term "public interest" being used as an exception in (e) can also cause significant issues as it is not defined in the Bill what would constitute as public interest in the context of this law. It would not be advisable to leave this interpretation upto the data controllers, who might use the absence of a clear definition against the data subject, or the Authority that does not have the power to define such terms. | It is strongly recommended that part (c) and (d) be omitted in their entirety.<br><br>With regards to "public interest", we advise that the Parliament provides a clear definition of the term to avoid any confusion and misinterpretation. |
| 25: Right to Prevent Processing Likely to Cause Damage or Distress | The terms "damage" and "distress" are vague and subjective. They have the potential to be interpreted in a number of different ways, which can cause inconsistencies in the implementation and application of the law.<br><br>In 25(1)(b)(ii), the word "unwarranted" is vague and seems misplaced. It causes confusion as to what the intention of the lawmakers was while drafting this section.<br><br>Section 25(2)(c) gives overbroad and arbitrary powers to the Authority and | The Parliament must clearly define the type of "damage" and "distress" that is covered in the ambit of this law. This could include damage to reputation, monetary damages, mental distress/ agony caused, etc.<br><br>We recommend that 25(1)(b)(ii) and 25(2)(c) be removed entirely. 25(3)(b) should also be omitted to ensure the data subject's full control over their data. |

| | | |
|---|---|---|
| | Federal Government that go beyond its powers of delegated legislation. Any exception falling under Section 25 must be laid down by Parliament and the Authority/ Federal Government may not be given a free pass to add exceptions and conditions as they wish. This also indicates a clear malice on part of the Government.<br><br>The first part of 25(3)(b) disregards the consent of the data subject, and grants power to the Authority to refuse the data subject's right to prevent processing of data likely to cause damage or distress. Furthermore, it also gives the Authority the power to determine whether the distress or damage is worth the protection of right this clause is extending. | |
| 27:<br>Right to Erasure | Section 27(1)(c) refers to section 23 subsection (2) in the Bill, which does not exist.<br><br>Section 27(1) places far too many conditions on the right to erasure, when in fact the consent of the data subject should be given the utmost priority.<br><br>In 28(1)(b)(ii)(b) and 28(1)(b)(iii), the term "vital interests" is included. As mentioned in Section 5.2, the term is vague and leaves room for misuse and misinterpretation. | We recommend that this section be clarified by adding reference to the correct section and subsection.<br><br>The conditions in this clause should grant more power to the data subject over their right to erasure, and should only include (a) and (b), whereas the rest of the conditions should be omitted.<br><br>Define "vital interests" clearly in the Definitions section. |

| | | |
|---|---|---|
| 29: Repeated Collection of Personal Data in Same Circumstances | The section infringes upon the rights of the data subjects guaranteed under the law and goes against the international standard of best practices set by the GDPR. Consent must be acquired every time data is collected. | We recommend that the section be omitted entirely. |
| 30: Exemption | In Section 30(2)(a)(f), the terms "journalistic", "literary" and "artistic" are not defined. All three terms can have a range of different meanings, which can cause confusion. | The legislature must define these terms to avoid ambiguity and confusion in the implementation of the law. |
| 31: Power to Make Further Exemptions | This section is unconstitutional, and gives overbroad and arbitrary powers to the Authority and Federal Government that go beyond the ambit of delegated legislation. Any exceptions made from this must be laid down by Parliament alone, and the Authority / Federal Government should not be given a free pass to add exceptions and conditions as they wish. This also indicates a clear malice on part of the Government. Only the legislature can make further exemptions as per Pakistan's constitutional law. | We strongly recommend that this entire section be removed altogether to ensure that the Federal Government and the Authority do not overreach and act in an unconstitutional way. |
| 32: Establishment of the Authority | Section 32(2) states that the Authority will be autonomous, while simultaneously being under the administrative control of the Federal Government. This section is inherently contradictory and has the potential of creating a conflict of interest when a public body or a | The Authority should be an independent body, and should not be influenced by the Federal Government, in order for it to effectively enforce data protection legislation in the country. Instead of the partial Authority envisioned under the Draft Bill, an independent |

| | | |
|---|---|---|
| | government department is undergoing investigation under the Personal Data Protection Bill once it has been passed.<br><br>Section 32(4) outlines the composition of the seven member Authority; all members would be appointed by the Federal Government. The appointment of government officials, including members of the Ministry of IT, Ministry of Defence, and Ministry of Interior, would severely hinder the purpose and implementation of data protection legislation, and will make the Authority dependent on government approval and susceptible to conflicts of interest and influence.<br><br>Section 32(9) lays out the requirement of the Authority members to not be employed anywhere else during their appointment within the Authority. While this would make sense from an administrative point of view, it will make the members of the Authority government employees, essentially bringing in yet another conflict of interest whenever and if a public body or individual is involved in the breach of citizens' data.<br><br>Section 32(12) gives powers of administration to the Chairman of the Authority, and also makes cross reference to section 38 to follow regulations that underline wide powers given to the Federal Government, thereby giving the Federal Government even more | Privacy Commission should be established, as proposed in the previous draft of the bill, while ensuring that its composition and functions align with international standards. The priority of this body should be to ensure independence in its functions, and transparency in relation to its implementation of the law.<br><br>The members of the Authority, especially the members from ICT, financial, legal and civil society sectors, should not be appointed as the employees of the Federal Government, and should remain autonomous in regards to decision-making. It should be ensured that in order to maintain the integrity of this implementing body, no skewed power dynamics exist between the members and the Federal Government.<br><br>The administrative powers should be at the disposal of the regulating/implementing body, and should remain independent from the interference of the Federal Government. |

| | | |
|---|---|---|
| | control over the Authority. This strips the regulating body (in this case, the Authority) of its independence, and leaves the decision-making powers at the discretion of the Federal Government. | |
| 34: Powers of the Authority | The Authority has been given the powers of a civil court in that it can propose penalties, but the procedure for this has not been laid down in much detail in the Draft Bill.<br><br>Moreover, Section 34(2)(i) lays out a schedule of cost for the registration of complaints. It puts the burden of the payment for registering a complaint on the data subject to seek protection of their data. | The creation of a new court takes time and a lot of parameters need to be prescribed under the law for this to happen. We are also concerned this Section underscores another means of giving the Authority, and the Federal Government, broad powers. Therefore, it needs to specify how this court will be established immediately after the Draft Bill comes into effect, and how it will work under the supervision of the relevant High Court.<br><br>Moreover, registering complaints should be free of cost for the data subject.<br><br>Section 46 of the Draft Bill should be amended accordingly. |
| 37: Meetings of the Authority | The quorum defined in Section 37(3) is problematic, as the 3 members required for a meeting of the Authority could very well be ex-officio members. only as per Section 32 of this Draft Bill (which, as mentioned above, is already in need of significant revisions). | At least 4 out of the 5 members should constitute a quorum for a meeting of the Authority. |

| | | |
|---|---|---|
| 38: Powers to the Federal Government to issue policy directives | This section grants sweeping powers to the Federal Government, which further affects the independence of the Authority, thereby blurring the lines that separate the Authority from the Federal Government. The Federal Government should not be intervening in the implementation of this regulation. This will also create a conflict of interest in the case of a data breach involving a government body or public department. | We strongly recommend deleting this section.<br><br>Moreover, there is another section 38 regarding Members and Employees; its numbering should be fixed for clarity's sake. |
| 39: Appointment of Employees | This section does not clearly define the criteria of selection of the employees, how they will be hired, and what training they will undergo before they are able to handle the powers vested upon them under this regulation. It leaves room for a lot of interpretation that could result in the employment of unqualified or unfit members within the Authority. | This section should clearly mention the appointment criteria and eligibility conditions, including the qualifications required, in regards to the selection and hiring of future employees, to ensure that proper procedures are followed based on predefined specifications, in order to leave little room for interpretation. Furthermore, it should also define the training the employees will undergo before exercising the powers underlined in the regulation. |
| 39: (mistitled) Cooperation with International organizations | The numbering of this section needs to be looked into, as there are currently two Section 39s in the Draft Bill.<br><br>This section mandates the Authority to seek approval of the Federal Government before cooperating with international organisations. Again, this seems like an attempt to strip the Authority of its autonomy, essentially leaving it at the behest of the Federal | Fix the numbering of this section, and the sections to follow, as there are currently three section 39s in the Draft Bill.<br><br>This section should empower the designated body to make decisions that do not require the Federal Government's approval as a priority. This section should also entail maintaining a public record of the cooperation to ensure that all |

| | | |
|---|---|---|
| | Government to make decisions on its behalf. | essential and non-essential information of this cooperation involving citizens' data is accessible to everyone, while not compromising on the said data. |
| 40: Funds | This Section does not specify how the Authority will retain financial independence from the Federal Government, considering the Federal Government will be the primary source for financing it, and will also be responsible for approving foreign grants and funding opportunities. | Explicitly state how the Authority will become financially autonomous in the long run, if not immediately, so it can execute its mandate effectively. |
| 41: Unlawful Processing of Personal Data | This section lays out the fine data processors are liable to pay in the case of the unlawful processing of data. In view of the penalty, we believe that whereas the fine of twenty five million rupees is a lot for small businesses and public bodies and departments, it is not enough for big businesses and corporations, and may not effectively hold them accountable for unlawful processing of people's personal data. | The law should create clear brackets, based on the scale and sensitivity of operations, for different kinds of entities and data processors, to ensure that the liabilities of data processors are appropriately defined. |
| 45: Complaint | Section 45(1) outlines the scenarios in which a complaint can be filed. However, the lack of definition of the term "relevant person" leaves it open to various interpretations, potentially creating a loophole or hindrance in the complaints mechanism.<br><br>Section 45(3) lays out the requirement of charging a fee to | The term "relevant person" needs to be precisely defined.<br><br>The requirement of a fee should be omitted. The complaints process should be free of charge. |

| | | |
|---|---|---|
| | process a complaint. This puts the financial liability on the complainant that will deter them from reporting non-compliance or breach of data protection. | |
| 46: Appeal | The establishment of the forum to hear appeals has not been laid out clearly. | The forum to hear appeals should be laid out clearly under the Draft Bill, and must come into effect immediately after this Bill comes into effect. |
| 48: Power to Make Rules | Section 48(1) empowers the Authority to make Rules, but it does so on the condition of seeking approval from the Federal Government. This, as pointed out earlier in Sections 32(12), 38 and 39 (mistitled), takes away the autonomy from the regulating body (i.e. the Authority), and gives the Federal Government unfettered powers. | It should be ensured that these powers should solely be vested in the regulatory body, instead of the Federal Government, to ensure autonomy and independent decision-making and effective implementation of the law. |
| 50: Removal of Difficulties | This section gives the Federal Government the power to remove difficulties by passing an order published in the Official Gazette. We believe that it is extremely important that these orders be presented before Parliament to make sure the Federal Government does not exceed the scope of its powers under this law while passing such orders. | The following subsection should be added to this: "Every order made under this section shall, as soon as may be after it is made, be laid before each House of Parliament." |

## Conclusion

We believe that upholding the rights of the citizens should be at the core of any national data protection framework. We appreciate the efforts of the Ministry in initiating a consultative process in relation to the draft Personal Data Protection Bill and hope that the Ministry will incorporate our recommendations to ensure that the rights of Pakistani citizens are respected and upheld. The Draft Bill needs to be clearer in terms of elucidating the scope of its application. Moreover, the most important aspect of any data protection law should be the establishment of an independent body that is free from government pressure in particular.

We hope that our recommendations are duly considered by the Ministry, and the Draft Bill is improved accordingly.


Policy Research & Advocacy Initiative