Asia Internet Coalition (AIC) Industry Submission on Pakistan Draft Data Protection Bill 2023

(Private Member Bill)

---

3 April 2023

Honourable Mr. Syed Amin Ul Haque
Federal Minister for Information Technology and Telecommunication
Ministry of Information Technology and Telecommunication (MoITT)
7th Floor, Kohsar Block, Pak Secretariat,
Islamabad, Pakistan

Cc: Honourable Prime Minister Muhammad Shehbaz Sharif, Prime Minister's Office, Islamabad, Pakistan

On behalf of the Asia Internet Coalition (AIC) and its members, I am respectfully submitting our recommendations on Personal Data Protection Bill 2023, which was moved by Senator Afnan Ullah Khan as a Private Member Bill before the Pakistani Senate on 13 February 2023 (the "**Bill**").

There are 16 core issues which have been identified in the Bill. Out of these 16 issues, the issues that have a material impact on the industry and business operations in Pakistan include: (1) the requirement to store personal data in Pakistan; (2) the regulator's power to expand on the list of what constitutes "sensitive personal data" and impose further conditions for the processing of sensitive personal data; (3) prohibitions on certain types of processing for personal data of children; (4) the absence of "legitimate interest" as a legal basis for processing personal data; and (5) the regulator's residual power to formulate specific regulations for "big/large data fiduciary/processors, along with other categories".

We find that the Draft Bill still does not address a majority of industry's substantive concerns such as stringent limitations on cross-border data flows and mandatory data localization, overbroad and vague definitions of key terms such as sensitive personal data and critical personal data, and globally divergent data subject rights, as well as far-reaching powers of the Commission. These provisions fall short of international standards for data protection (such as GDPR) and will adversely impact Pakistani consumers and businesses. In its current form, the Bill will have a negative impact on the ability of foreign internet companies to trade with and operate in Pakistan, hindering the country's economic recovery and deterring foreign investment. Local Pakistani companies may lose access to cost-efficient global cloud services making them less competitive as they incur substantial costs to operate and maintain servers.

The protection of personal data is an important component of any privacy framework, and we appreciate the opportunity to provide feedback on the Draft Bill. AIC and its members have worked closely with governments around the world in relation to the development of national personal data protection policies and legislation. In doing so, we have witnessed first-hand the potential for such policies and legislation to effectively protect the privacy interests of citizens without hindering innovation and technological advancement. We recognize the on-going efforts of the Government of Pakistan and the Ministry of Information Technology and Telecommunications ("**MOITT**") in further fine-tuning the draft legislation, but we continue to have concerns, particularly on cross-border transfer of "critical" and "sensitive" personal data.

On this note, the AIC wishes to request for an industry meeting to better understand the views and priorities stemming from the Bill. This introductory meeting can also discuss potential areas of collaboration as well as opportunities for consultation that can further assist the Government's review of the Personal Data Protection Bill 2023. As such, we welcome a video conference meeting with you or your team at a date and time of your convenience.

Importantly, we trust that these comments and recommendations are useful and look forward to working closely with the Government of Pakistan, other industry players, consumer groups and all other relevant stakeholders to help deliver an effective and robust privacy framework for Pakistan based on international good practices.

Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

---

1. Definitions of "personal data", "critical personal data" and "sensitive personal data"

- The Private Member's Bill does not have a definition of "personal data" so the nature of data/information to which the Bill applies is not clear. We propose a scope of "personal data" that is clear and not overly broad to reduce business uncertainty.
- The definition of "critical personal data" covers (i) unregulated e-Commerce transactions, which is undefined; (ii) data related to public service providers; and (iii) data related to international obligations, which is also undefined. This definition is overly broad and ambiguous, creating significant uncertainty for businesses. The special care category of "critical personal data or CPD" is unclear and should be entirely removed. *As the objective behind inclusion of this special-care category is unclear, and the contours of what would constitute CPD are broad and ill-defined, organizations will face operational difficulties in complying with the Private Member Bill.*
- The definition of "sensitive personal data" still contains certain forms of non-personal data, such as passwords. This definition is overbroad and exceeds international best practice. The definition of SPD is too broad and the grounds for processing SPD are too narrow – We recommend *excluding "financial data" and "official identifier" from the scope of Sensitive Personal Data*

(SPD) and increase the list of grounds for the processing of such data, in line with international best practices.

Specifically on Sensitive personal data (Section 3(gg) and Chapter IV of the Bill), we recommend the following:

a. Align the definition of sensitive personal data with global privacy law norms such as the EU's General Data Protection Regulation;
b. the Commission's power to designate further categories of data as sensitive personal data should be deleted; and
c. the conditions for processing sensitive personal data should be clarified.

Sensitive personal data is a concept common to most international benchmark data protection laws. These laws recognise that some information is of a particularly sensitive nature. Typically, the sensitivity arises from the fact that sensitive personal data reveals highly private aspects of a person, such as their race, religion or political opinions, and usually these are aspects that cannot be changed by a person.

Overall recommendations for Section 3

- 3(g): remove definition of data, which is non-standard and goes beyond the scope of the law. We Suggest introducing a definition of personal data instead, aligned with best practices in data protection law.
- 3(h): remove definition of data breach, since there is already a definition for personal data breach under (x)
- 3(k): revise definition to mean simply the person to whom the personal data relates. The parents or lawful guardians of a child should not be considered data principals as a result.
- 3(s) and (ii): remove intersex status and transgender status from the data protection law. This could be seen as detrimental to fundamental rights where organizations would seek to obtain such data, and is not part of international data protection laws. The notion of sensitive personal data would already cover those to the extent they need special protection.
- 3(aa): definition of profiling is overly broad and should be at least limited to circumstances involving automated processing
- 3(bb): there are concerns about the swiping definition of public interest here, in particular regarding (v) and (vi)
- 3(gg): overly broad definition of sensitive personal data. We suggest using the standard of the GDPR, which is widely adopted. In particular, passwords, financial data, official identifier are not pieces of data that would be considered sensitive data under modern data protection law. These restrictions would make it difficult for businesses to operate in Pakistan.

1.1. <u>Align definition of sensitive personal data with global privacy norms</u>

The Bill's inclusion of passwords and financial data in the definition of sensitive personal data goes beyond accepted global norms. The definition of "sensitive personal data" should only include information that is by nature of a higher risk to individual privacy. For ex. passwords may not in some cases even be able to identify an individual let alone present sensitive information about an individual. It is also recommended that the reference to financial data be removed from the definition of "sensitive personal data" for this reason. Not all types of financial data are always at higher risk to individual privacy and so a blanket inclusion of financial data would not be proportionate to the increased protection provided to such sensitive personal data. For example, a

person's credit history may be more sensitive in certain circumstances, but the fact that he/she has opened a bank account with a particular bank may not be. In this context, it is understood that financial data is separately controlled by the State Bank of Pakistan which has recently issued BPRD Circular No. 4 of 2020 allowing financial institutions to outsource hosting on the cloud to both domestic and international cloud service providers (and thereby disclose financial data to such third parties). Therefore, to ensure consistency between financial sector regulations and the general law, financial data should not be subject to separate sensitive personal data requirements under this Bill.

1.2. Delete Commission's power to designate further categories of sensitive personal data

Section 20 of the Bill empowers the Commission to designate further categories of personal data as sensitive personal data. This generates significant uncertainty around compliance obligations for organisations. The uncertainty is also not advantageous to data principals who look to data privacy legislation to be educated on, understand and manage their privacy rights.

1.3. Conditions for processing sensitive personal data should be clarified

As currently drafted, Section 17 of the Bill appears to contemplate permitting sensitive personal data to be based on the data principal's "explicit consent", but this concept is not elaborated further in the body of the section (instead, reference is made to the processing of sensitive personal data in connection with government-related functions). For greater clarity, the Bill should be amended to permit the processing of sensitive personal data based on explicit consent and include a definition of what this concept entails (for instance, it could define explicit consent as an express statement of consent given by the data principal, which is consistent with global benchmark definitions, such as the European Data Protection Board's Article 29 Working Party guidelines on consent).

Additionally, the Commission is empowered under Section 20(2) of the Bill to prescribe further protections or restrictions on the processing of sensitive personal data where the repeated, continuous or systematic collection of such data for profiling takes place. The current drafting in the Bill lacks the necessary specifics to make it clear for organisations what these additional protections or restrictions are and how they should comply with those requirements. While there is some merit in giving the Commission the flexibility to prescribe further rules on the processing of sensitive personal data, the lack of general principles at the primary legislation level creates confusion and uncertainty. As explained above, this is not advantageous for organisations and data principals, who both look to data privacy legislation to understand and manage their privacy rights and obligations.

2. Data localisation and cross-border data flows (Sections 30 and 31, Bill)

- The Private Member's Bill does not address earlier industry concerns such as stringent limitations on cross-border data flows and mandatory data localisation. The Bill appears to impose a broad data localisation mandate on all personal data. Section 30(1) of the Private Member's Bill reads: "Every data fiduciary shall ensure personal data is stored on a server or data centre based in Pakistan." While both previous and the latest MOITT Draft Bill provide certain additional legal bases for the cross-border transfer of personal data (e.g. explicit consent/binding contracts/international cooperation), the Private Member's Bill only enables cross-border transfer

if it is determined that the jurisdiction to which data is being exported offers equivalent protection.

- While there is a provision for the Commission to grant exemptions for certain categories of data from this general data localisation provision, overbroad and vague definitions of personal data and broad data localisation mandate fall short of international standards for data protection (such as GDPR) and will adversely impact Pakistani consumers and businesses.
- Forced data localisation harms businesses and is not conducive to privacy and security protection.

    - Forced data localisation harms businesses from every sector and stifles trade. Most businesses today rely on data to manage global operations, and data flows contribute significantly to economic growth and digital trade. The inability to move data freely across geographies creates a major impediment to efficiency, productivity, and costs.

    - Requiring that data be exclusively stored in one location may put users' privacy and security at greater risk. Distributed networks are built to be resilient and to allow for redundancy in the event of a network failure. Data localisation requirements typically increase data security risks, privacy risks, and costs by requiring storage of data in a single centralised location that is challenging to maintain and less likely to be updated to follow security best practices.

We, therefore, recommend the following:

a. Remove the requirement to store personal data on a server or data centre in Pakistan under Section 30(1) of the Bill; and
b. remove the prohibition on the transfer of critical personal data and "some components of sensitive personal data" outside of Pakistan under Section 31 of the Bill. If the policy concern is for data pertaining to national security not to be transferred overseas, then the transfer prohibition above should be limited to government-held data.

Pakistan's economy will benefit from unimpeded cross-border data flows ("**CBDFs**"). In contrast, data localisation (in the form of requirements to store data in Pakistan or prohibitions on the transfer of data outside of Pakistan) will stifle the economy and chill foreign investment. Data localisation will also heighten cyber security risks.

2.1. Pakistan's economy will benefit from unimpeded CBDFs

Cross-border data flows are essential to growing Pakistan's economy and ensuring Pakistani businesses remain competitive in the global economy. Embracing cross-border data flows will: promote productivity, innovation, and efficiency; lower costs for consumers and businesses; lower barriers to international trade and investment; increase access to global products and services; and ensure Pakistani businesses can service consumers at home and abroad.

Economic modelling and independent analyses illustrate the value of embracing CBDFs. Increased CBDFs grew global GDP by 10% ($2.8 trillion) in 2014, with emerging digital markets standing to benefit from 50% GDP growth by embracing CBDFs. These potential gains have grown significantly as the amount of data that transits global networks has since multiplied exponentially [McKinsey 2016].

2.2. Data localisation will have a chilling effect on foreign direct investment

Data localisation requirements reduce foreign direct investment and restrict the availability of services to local consumers. Multinationals looking to invest may forgo Pakistan in favour of markets with less burdensome costs of entry. In fact, the US National Trade Estimate identified restrictions on data flows and data localisation requirements as a leading impediment to foreign direct investment by US companies [USTR 2020].

The World Economic Forum's recent report on data flows warns that data localisation requirements chill e-commerce, destabilise supply chains, stifle the development of domestic talent, increase compliance costs for SMEs, and cause "local companies and consumers [to] lose access to cloud computing capabilities and other advanced foreign information technologies, pay higher prices and become uncompetitive in global markets" [WEF 2020]. Evidence suggests that, in China, the government's restrictive approach to data flows and data localisation requirements have caused economic harm and limited growth potential. For example, in Oct 2021, LinkedIn announced that it will close its service in China due to the more "challenging operating environment." following China's passage of the Personal Information Protection Law (PIPL) [NYT 2021].

2.3. Data localisation heightens privacy and security risks

Requiring that data be exclusively stored in one location or in one country puts users' data at greater risk by centralising data storage and creating a "honey-pot" of data that is vulnerable to unauthorised access and cyber attacks. In contrast, distributed networks are built to be resilient and allow for redundancy in the event of a network failure to ensure business continuity for organisations. Global companies, and particularly technology-dependent companies, rely on cloud storage solutions for their data management because it allows for an affordable and scalable way to deploy the latest technology and tools across the network to make it secure. This is not possible with data localisation.

3. Processing data relating to children (Sections 3(c) and 15 of the Bill)

We recommend:

a. For the purposes of this Bill, the definition of "child" should be changed to a person who has not attained the age of 13; and
b. remove age verification, parental consent and child-related data processing prohibitions in the Bill – the better approach may be for the industry to work with the Commission in preparing Codes of Practice to cover such matters.

The age of consent as it applies in the context of accessing online services should be distinguished from the age of majority as it applies in the context of drinking alcohol, consenting to sexual intercourse, voting, or criminal liability, where decidedly different policy considerations are taken into account. An increasing number of teens are developing digital literacy and have significant online presence, with a large majority of them more conversant with technology and related issues than their parents, and so it is important for the legal framework to recognize their autonomy to make decisions for themselves. In many jurisdictions, the age of consent for accessing online services is much lower than other statutory age of majority, and where parental consent is required, it does not serve as a complete bar to accessing the service. Furthermore, the internet is home to a wealth of educational material which Pakistani youth may be denied access to if such organisations decide to geo-block their offerings from being accessed in Pakistan. Being unable to access

and benefit from these extensive educational resources due to prescriptive consent requirements and age restrictions would undoubtedly disadvantage Pakistani youth in comparison to their peers from other countries.

Additionally, imposing prescriptive age verification, parental consent mechanisms or processes and broad child-related data processing prohibitions could be unduly prohibitive and may not be appropriate to the specific circumstances of data collection or processing. For example, if certain technological measures must be implemented, these may be onerous for smaller businesses that target children (e.g. local toy stores or educational websites) and may stifle innovation by smaller, local companies in Pakistan. It is important to also note that parental consent does not in itself prevent exposure to harmful content online; in practice, this is achieved through the implementation of special protections. Instead of having the Commission impose age verification, parental consent requirements and child-related data processing prohibitions, the better approach may be for the industry to work with the Commission in preparing Codes of Practice around verification processes. As industry standards evolve and become more robust, so can the Code of Practice. Given that verification mechanisms are technical and industry best practices around it evolve constantly, it is important to adopt a co-regulatory, multi-stakeholder approach to find the right solution to this.

4. Consent for data processing (Section 6 of the Bill)

We strongly recommend, permit processing of personal data without consent where it is in the legitimate interests of the data fiduciary.

There are various exceptions to consent set out in Section 6(6) of the Bill, but the section does not contain an exception which permits personal data to be processed without consent where it is in the legitimate interests of the data fiduciary.

While consent is an important feature of any privacy law framework in that it alerts data principals to the fact that their data is being processed, there is a risk of consent fatigue developing if data principals are repeatedly asked to provide consent each time their personal data is being processed, particularly where the risk of harm arising out of the processing activity is minimal. To address this problem, more exceptions to consent should be introduced in the Bill. For instance, an exception to permit the processing of personal data without consent where it is in the "legitimate interests" of the data fiduciary could be introduced, which aligns with the approach adopted under international benchmark legislation such as the GDPR. To mitigate against the risk of the legitimate interest exception being abused by data fiduciaries, safeguards can be put around this exception, such as requiring the data fiduciary to undertake an internal balancing exercise to ensure that the risk of harm to the data principal does not outweigh the legitimate interest being pursued. While it should be noted that Section 5(2) of the Bill makes reference to the concept of "legitimate interest", the concept is used to establish principles applicable to the lawfulness of processing, rather than operating as a legal basis or consent exception used to justify the processing of personal data.

5. Registration framework for data fiduciaries and data processors (Section 40(2)(e) of the Bill)

We recommend that the Commission's power to implement a registration and licensing framework for data fiduciaries and data processors should be deleted. *Registration requirements generate administrative burdens on the data protection authority and increase the cost of operations for both the regulator and regulated organizations, whilst not offering additional levels of protection to personal data.*

Implementing a registration and licensing framework would be out of step with most regional laws and international benchmarks including the OECD Privacy Guidelines, the GDPR, Singapore's PDPA and Australia's Privacy Act. This would be an unnecessary administrative burden for the government, increase compliance costs for organisations (particularly if registration fees and annual fees are imposed), and may not lead to a meaningful increase in compliance by organisations or enhance privacy protections for data principals.

Furthermore, given the nature of the internet and accessibility of almost any website by users in Pakistan, this may result in international companies and services pre-emptively geo-blocking their services from the Pakistan market so as not to be subject to the registration requirement, which would undoubtedly result in less choice and benefits for consumers. In any case, registration does not necessarily lead to meaningful compliance by organisations because even if offshore organisations do register with local regulators, the practical challenges of enforcement against offshore entities still remains, together with the ongoing risk of organisations geo-blocking their services from Pakistan as highlighted above.

6. Notice (Section 8 of the Bill)

We recommend, removing the phrase "itemised notice" from Section 8(1)(a) of the Bill. The Commissioner's power to prescribe further information to be included in the notice under Section 8(1)(i) of the Bill should also be deleted.

The requirement to provide an "itemised notice containing a description and categories of personal data sought to be collected" is too prescriptive and may result in notice fatigue for data principals if the expectation is for an extensive amount of detail to be provided for the "itemised notice". A data principal could suffer from notice fatigue if he or she were to be presented with an extremely long list of personal data that is sought to be collected by the data fiduciary. Given that the Bill is structured in a manner where consent is the primary legal basis for processing personal data subject to the consent exceptions in Section 6(6) of the Bill, and that notice is a precursor to consent (in that the data principal cannot consent to the specific purposes for processing personal data without those purposes first being notified to him or her), the consent obtained as a result of notice fatigue (where the data principal blindly accepts the purposes for which his or her personal data is processed) would not necessarily be meaningful. In this context, it is questionable if the consent given by the data principal is a specific, informed and unambiguous indication of his or her assent to the data processing. Ultimately, privacy laws should not prescribe in detail the manner in which notice is to be provided to data principals because the type of notice that is appropriate will depend on the context. It would be sufficient for Section 8(1)(a) to set out a general requirement for data fiduciaries to provide a description of the personal data sought to be collected, without further specifying how this should be presented.

Additionally, the Commissioner's power to prescribe further types of information that needs to be included in the notice under Section 8(1)(i) of the Bill should be deleted. There is limited merit in giving the Commission the power to prescribe additional information that needs to be included in privacy notices, as the content of the privacy notice is not expected to evolve over time or with changes in technology. The lack of fixed notice requirements at the primary legislation level is not ideal as it is likely to lead to confusion and uncertainty. As explained above, this is not advantageous for both organisations and data principals, who look to data privacy legislation to understand and manage their privacy rights and obligations.

Further Section 8)2)b) appears to be incompatible with (a). We seek further clarification in which cases post-collection notice is acceptable under the law.

7. Security requirements (Section 10 of the Bill)

We recommend that the requirement for the Commission to prescribe practices for protecting personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration, or destruction should be deleted.

Effective personal data protection legislation should be technology-neutral to both cater for the diverse way that personal data is currently handled (e.g. offline and online methods) and for future technologies that have yet to be developed. Prescriptive security standards are arbitrary, increase compliance costs for organisations, and may not always result in tangible benefits for the data principal. The measures taken to protect personal data should be proportionate to the nature of the personal data and the types and purposes of processing. There is no "one-size-fits-all" solution. For example, a small store running a simple offline membership loyalty program cannot be expected to implement the same security controls to protect the personal data it collects as a healthcare company that deals with thousands of patient records every day.

Therefore, there should be flexibility for organisations to decide what security controls are suited for the types of personal data, processing activities, and based on best industry practice. Section 10.2 of the Bill already requires that the security measures implemented be appropriate to protect personal data from security incidents. This requirement would already be sufficient and is consistent with global privacy norms.

Section 10)(1) is an additional and unnecessary obligation to (2). Also, data security practices should not be affected by national interest or be prescribed by regulators, as the bill already provides for the need to employ technical and organizational security standards. It should be for the data fiduciary to ensure this is delivered.

8. Data retention requirements (Section 11 of the Bill)

Flexibility should be built into the requirement to delete and destroy personal data if it is no longer required for the purpose for which it was to be processed, and further exceptions to address situations where personal data must be retained for legal and/or audit purposes should be included.

Additional provisions should be included to provide organisations with flexibility and exceptions where there are technical limitations and personal data cannot be deleted and destroyed in a prescriptive timeframe. In particular, where an organisation holds automated backups of data that are scheduled to be deleted, destroyed or de-identified, this should be sufficient enough to demonstrate compliance with this retention limitation requirement.

The Bill should also provide enough flexibility so that deletion or destruction of data is not required where it is not technically feasible to comply, where deletion/destruction would prevent organisations from performing a contract or providing a service requested by a user, and where the data must be retained for disaster recovery or legal/compliance purposes. To accommodate this, inspiration can be taken from Singapore's Personal Data Protection Act ("**PDPA**"), which permits organisations to retain personal data where it is necessary for any legal or business purposes.

9. Personal Data Breach Notification (Section 14 of the Bill)

We recommend introducing a phased approach to the provision of prescribed details to be included in a personal data breach notification to the Commission and data principals under Section 14(3) of the Bill, or alternatively, provide for a much longer timeline for notification to the Commission and data principals (e.g. 1 week).

The Bill includes a requirement to notify both the Commission and data principals of any personal data breach, unless such breach is unlikely to result in an infringement to their rights and freedoms within 72 hours. While timely notification of such data breaches is important, it is more important that organisations are able to present the facts of the breach fully and accurately. It takes time to evaluate the nature and scope of a breach and assess the likely harm caused, and therefore privacy laws should give organisations adequate time to carry out the tasks identified above before making a notification. The notification of breaches based on incomplete or inaccurate information makes the notification process less meaningful. Additionally, there is a risk that inaccurate or multiple breach notifications (to correct inaccuracies in previous breach notifications) could potentially strain the resources of the Commission as it would need to investigate or respond to every notification, including ones that may ultimately prove to be low risk, but which had initially been notified to the Commission based on an incomplete assessment.

Therefore, a phased approach (which permits organisations to provide the prescribed details to be included in a personal data breach notification progressively in phases, and not immediately once the 72 hour deadline is reached, provided that such information was not available at that time) would allow for more accurate details to be presented as investigations give a fuller and more accurate picture of what happened. To safeguard against the risk of organisations taking advantage of this phased approach to unduly cause delay to the notification, the Bill can require that information be provided without undue delay as soon as it becomes available.

As an alternative, if a phased approach cannot be adopted, it may be worthwhile to consider a much longer timeline for notification (e.g. 1 week), to allow sufficient time for the organisation to adequately assess the breach and provide accurate and complete information to the Commission and data principals.

Section 14(5) should be removed. The data processor shall not have obligations in relation to data breach notifications other than informing the data fiduciary about any events it becomes aware of during the processing.

10. Right to erasure (Section 25 of the Bill)

(1) There should be more flexibility built into the timeframe for complying with a data principal's request to erase personal data; and (2) the qualification at the start of Section 25(3) that the application of the exceptions to the right of erase only apply where they do not prejudice the rights of the person protected under the Bill should be deleted.

The data fiduciary has an obligation under Section 25 of the Bill to erase personal data within a period of 14 days. These timelines are unreasonably short and would pose a significant, if not insurmountable, administrative burden for businesses, in particular small enterprises. The prescriptive timelines should be removed and replaced with an obligation to respond "as soon as reasonably possible" or "promptly" to recognise that different cases require different response times, depending on the complexity of the request,

while still ensuring the organisations prioritise such requests. For example, Article 12 of the GDPR affords data controllers one month to respond to a request and this can be extended by a further two months.

Additionally, the exceptions to the right to erasure in Section 25(3) of the Bill are subject to a vaguely worded condition that the reliance on the exceptions do not "[prejudice] the rights of the persons protected under the Act". This condition implies that data fiduciaries must now conduct a balancing test before they can rely on any of the listed exemptions, in order to ensure that the rights of any person (and not just the data principal) are not prejudiced. Furthermore, the scope of this balancing test is unduly vague since it is unclear what conduct would be considered to prejudice the rights of a person under the Bill.

11. Notification of data processing to Commission (Section 13 of the Bill)

The requirement to notify the Commission of all collection and processing activities should be removed.

Whilst requiring organisations to maintain internal records of personal data processing is important to foster transparency and accountability within an organisation and is a feature of a number of international benchmarks including the GDPR, an ongoing requirement to regularly report to the Commission the types of data collected and the processing activities undertaken is burdensome to both the Commission and each organisation.

The exception to the notification requirement in cases where "data collection is occasional unless the processing results in the infringement of the fundamental rights and freedoms of the data principal, as enshrined in the Constitution of Pakistan" is not helpful, as a data fiduciary will need to assess whether its data collection is occasional, and conduct a balancing test, before it is able to determine if the exception applies. Furthermore, the scope of this balancing test is unduly vague since it is unclear what conduct would be considered to be an infringement to the fundamental rights and freedoms of the data principal as enshrined in Pakistan's Constitution.

Section 13) (1) proposes an overly broad record keeping obligation. It is also concerning that there would be additional regulations on how records are to be kept. This is not in line with modern data protection laws.

12. Regulations for big/large data fiduciary/processors (Section 40(2)(d) of the Bill)

The Commission's power to formulate specific regulations for "big/large data fiduciary/processors, along with other categories" should be deleted.

It is unclear what definition will be applied to "big/large data fiduciary/processors, along with other categories" and what additional restrictions will be imposed on such organisations, therefore generating significant uncertainty around compliance obligations for businesses of all sizes. Privacy laws should in general adopt a consistent approach to privacy and imposing additional restrictions based on the size of the data fiduciary or processor would be arbitrary and may not result in greater protection for data subjects. The nature of the personal data and processing is far more relevant to protecting the personal data and privacy of data subjects than the scale.

13. Fines (Chapter VIII of the Bill)

We recommend reducing the quantum of fines and focus instead on developing enforcement strategies that foster trust between the regulator and the regulated (e.g. informal engagement efforts by the regulator or formal warnings). Punitive sanctions should be used as an enforcement mechanism of last resort.

The quantum of fines for non-compliance with the provisions of the Bill is high. The provisions in Section 47(1) of the Bill permit a fine of up to 1500 million rupees (approx. USD 5.5 million) for processing, disseminating or disclosing personal data in violation of the Bill, and in the case of subsequent violations, the fine may be raised to up to 2500 million rupees (approx. USD 9.3 million). In cases where the violation relates to the sensitive personal data, the fine may be raised to the higher of up to 2% of the organisation's global turnover for the preceding fiscal year or 5000 million rupees (approx. USD 18.6 million).

Additionally, a fine of up to 500 million rupees (approx. USD 1.8 million) can be imposed for: (1) a failure to comply with the orders of the Commission or court when required to do so; (2) a failure to respond to a notice from the Commission to provide reasons for why an enforcement order should not be issued against the organisation, and (3) a failure to adequately explain an alleged contravention to the Commission and remedy such contravention within the time allotted by the Commission.

While enforcement frameworks are a necessary part of privacy laws, best practice in developing such enforcement frameworks strongly suggests that a carefully calibrated enforcement strategy helps to promote compliance. Specifically, leading international frameworks, such as the GDPR and the Singapore PDPA, focus on the key principles of fairness, proportionality, accountability, constructive engagement, and mutual trust. Successful enforcement strategies are those that focus on fostering trust between the regulator and the regulated, promoting accountability mechanisms such as codes of practice, and cautiously using punitive sanctions only as a last resort.

14. Definition of "fiduciary" (Section 3(l) of the Bill)

We recommend deleting the definition of "fiduciary".

The Bill's separate definition for "fiduciary" (in addition to the definition of "data fiduciary") is out of step with the controller/processor distinction used in other international benchmark laws. The concept of a "fiduciary" exercising rights and powers belonging to a principal is also not a commonly found concept in international benchmark laws, and so this could create confusion for international organisations operating in Pakistan. This could potentially lead to the unintended effect of non-Pakistan based companies geo-blocking some or all of their services and resources so that they will not be accessible to Pakistani users, as a precautionary measure to avoid inadvertently taking on additional measures as a "fiduciary" under the law. In any case, there is an overlap between the definitions of "data fiduciary" and "fiduciary", and this creates further confusion as to what constitutes a data fiduciary regulated under the Bill. The definition of "fiduciary" in the Bill considers the fiduciary to be an agent of a principal, but this is not necessarily a reflection of every single relationship between a data fiduciary and a data principal (as such data fiduciary-data principal relationships could include service provider-customer and employer-employee relationships). There is a risk that definitional ambiguity could result in certain types of "controller" organisations falling outside of the definition of a data fiduciary and accordingly not being subject to the provisions of the Bill.

15. Data processing exemptions (Sections 29, 32 and 33 of the Bill)

We recommend moving the data processing exemptions under Sections 29, 32 and 33 of the Bill to a separate chapter on "Exemptions".

As it is currently drafted, the Bill lists the exemption from the notice and consent obligations for repeated data collection under both the "Data Principal Rights" (see Section 29 of the Bill) and "Transfer of Personal Data Outside Pakistan" (see Section 33 of the Bill) chapters. The "exemptions" under Section 33 of the Bill appear to be general exemptions to the Bill's notice, consent and disclosure obligations but they are listed under the "Transfers of Personal Data Outside Pakistan" chapter. This is taxonomically confusing and there is a risk that with the current drafting, the exemptions will be read differently/more narrowly than what was originally intended by the drafter.

16. Extraterritorial application (Section 2 of the Bill)

The extraterritorial application of the Bill should either be deleted or aligned with international benchmarks, such as Article 3 of the EU's General Data Protection Regulation ("GDPR").

The Bill states that it applies "where any data fiduciaries or data processors not having a physical presence within the territory of Pakistan carries out the processing of personal data, if such processing is – (i) concerning any commercial or non-commercial activity offering goods or services to data principals; or which involves profiling data principals within the territory of Pakistan". This provision is wider as compared to Article 3 of the GDPR, which applies to controllers or processors located outside of the EU only where certain narrow thresholds are met (i.e. where the entity is actually offering goods or services to data subjects in the EU, or monitoring their behaviour). By extending the jurisdictional scope to include also foreign entities engaged in "non-commercial activity offering goods or services to data principals" (and the current drafting does not make it expressly clear that data principals must be located within the territory of Pakistan), the Bill goes further than the GDPR.

A clearly defined jurisdictional scope is important for both organisations and data principals who seek to understand and manage their privacy obligations and rights. The expanded scope of the Bill may have the unintended effect of causing non-Pakistan based companies to geo-block some or all of their services and resources so that they will not be accessible to Pakistani users, as a precautionary measure to avoid inadvertently infringing the law. This will result in fewer benefits and choices to individuals and companies in Pakistan. If despite these concerns, the extraterritorial application of the Bill is retained, then the provision above should be aligned with the position under international benchmarks such as the GDPR (including the clarifications in Recital 23 of the GDPR regarding what constitutes the offering of goods and services), so as to include clearly defined thresholds regarding the extraterritorial processing of the personal data belonging to data principals located in Pakistan.

17. Additional Comments:

- Section 47)(2): Fines should be limited to the national turnover (revenue generated within Pakistan), as it is not reasonable otherwise.
- Section 50)(1)(2) Excessive fines: The data fiduciary should be always allowed to challenge the orders and rules before a court of law before any such penalties are imposed.
- Section 52) There should be at least 12 months for compliance before the law is in force.