Asia Internet Coalition (AIC) Submission on Pakistan's Data Protection Bill 2021

---

22 September 2021

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

Subject: Asia Internet Coalition (AIC) Submission on Pakistan's Data Protection Bill 2021

Dear Minister Syed Amin Ul Haque,

On behalf of the Asia Internet Coalition ("AIC or We") and its members, I am respectfully submitting our recommendations regarding the Pakistan Personal Data Protection Bill 2021 that was published on 25 August 2021 (the "**Draft Bill**").

The protection of personal data is an important component of any privacy framework, and we appreciate the opportunity to provide additional 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 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.

Properly constituted data protection legislation has the potential to provide reliable standards for businesses and consumers and ensure the secure and responsible handling of personal data. As Pakistan's digital economy continues to grow, it is important that the country's privacy laws take into consideration three key goals: (1) the value of data protection in enabling a dynamic digital economy that protects consumers and facilitates Pakistani enterprise; (2) the need to promote data-driven innovation; and (3) consistency with global standards for data protection, such as the European Union's General Data Protection Regulation ("**GDPR**"), Organization for Economic Co-operation and Development ("**OECD**") Privacy Principles, and Singapore's Personal Data Protection Act ("**PDPA**") (together, examples of "**International Benchmarks**").

We trust that these comments and recommendations are useful and look forward to working closely with MOITT, 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)

Cc:

- Mr. Shoaib Ahmad Siddiqui, Federal Secretary, Ministry of Information Technology and Telecommunication
- Mr. Sher Afgan Khan, Additional Secretary, Ministry of Information Technology and Telecommunication (MoITT)
- Mr. Syed Junaid Imam, Member IT, Ministry of Information Technology and Telecommunication (MoITT)
- Mr Babur Suhail, Member Legal, Ministry of Information Technology and Telecommunication (MoITT)
- Bilal Abbassi, Director IT, Ministry of Information Technology and Telecommunication (MoITT)

OVERVIEW OF COMMENTS AND RECOMMENDATIONS

The Asia Internet Coalition submits the following suggestions, so as to ensure that the Draft Bill serves the interests of users as well as Pakistan's digital ambitions and goals.

- Reconsider the extraterritoriality provision. We are concerned that the Draft Bill's extraterritorial application is based on provisions that are too wide and vague, which would even bring within scope foreign companies that neither operate in Pakistan nor process data collected in Pakistan. The extraterritoriality provision goes beyond the provisions on applicability set forth in the EU GDPR.
- We seek clarity on the definition of sensitive personal data. We recommend that "access control data" and "financial information" are excluded from the ambit of 'sensitive personal data,' which would be in line with international best practices and in the interests of the digital services sector in Pakistan.
- We recommend removing mandatory data localization requirements. At present, the Draft Bill includes an extremely broad data localization requirement that will impose significant burdens on all businesses operating in Pakistan. We note with concern that the categories of "critical personal data" and "some sensitive data" remain broad, which makes it difficult for companies to plan their business. Besides being a bad security practice that incentivizes attacks by bad actors by creating a single attack surface and point of failure, data localization will result in increased data storage costs that will likely be passed on to Pakistani consumers. Contrary to popular belief, data localization will not necessarily result in better law enforcement outcomes because the underlying conflict of laws that restricts the ability of U.S. service providers to disclose data will remain in place regardless of the location of data storage. Moreover, by instituting a data localization requirement, Pakistan would be endorsing measures that undermine a vital source of its own growth and innovation. We hope that Pakistan and the United States work towards facilitating cross-border data flows between them.
- We recommend restricting consent requirements to new purposes of processing only. The requirement to obtain distinct indications of consent from users for each separate purpose of data processing will result in a flood of consent notices to users. This will neither increase transparency nor result in better data protection outcomes. Instead, it will instead create 'consent fatigue' among users and also overburden companies with a bureaucratic requirement that will disrupt the smooth functioning of Pakistan's digital economy.
- We propose reforming excessive penalties. The Draft Bill's monetary fines and its provisions creating criminal liability are excessive and will deter companies from doing business in Pakistan. Criminal liabilities, in particular, may deter constructive cooperation between data controllers and Pakistan's

future data protection authority. We believe that a greater emphasis should be put on accountability measures as a powerful factor to minimize privacy risks and encourage better data protection outcomes.

- We seek clarity on the requirements regarding DPOs. We request clarity in the Draft Bill regarding the obligations pertaining to the appointment and functioning of Data Protection Officers.
- The uncertainty surrounding the powers of the Commission should be removed. We recommend that the Draft Bill is revised to remove the Commission's powers to register and license data controllers, which would be a resource-intensive and time-consuming exercise without proportionate gains. Moreover, pursuant to our recommendation for the Commission to adopt a consistent approach to data protection, we believe that categorising companies into "big/large data controllers" is vague and unnecessary, and should be removed.

DETAILED COMMENTS AND RECOMMENDATIONS

1. **Requirements for data localisation and the concept of "critical personal data" should be removed**

AIC recommends that the Government remove all data localization measures within the PDPB, including requirements that: a) "Critical personal data" only be processed in a server or data centre located in Pakistan (Section 14.2) and b) the Commission devise a mechanism for keeping some components of sensitive personal data in Pakistan (Section 15.2). Data localization is an ill-advised policy, as data localization is a barrier to international trade and investment and will likely degrade the security of Pakistani citizen's data. Localisation obligations would also make it difficult for growing businesses in Pakistan to compete in global markets. For example, it would make it difficult for companies to gain access to innovative technologies that depend upon cross border data flows such as data analytics, AI/ML tools, etc. They may also lose access to cost-efficient cloud services in the global market. Therefore, we recommend such restrictions are eliminated to promote local business predictability and opportunities.

Additionally, Section 15.2 requires the Commission to introduce a data localisation framework to force companies to store some sensitive personal data in Pakistan, where necessary for public order or national security reasons. It is unclear what "some sensitive personal data" is defined as, which will confuse local businesses and deter foreign investors who seek to comply with this regulation. Furthermore, segregation of data into sensitive, personal or critical data in order to give them special treatment, such

as local storage, is technically not feasible for many businesses, particularly local and small to mid-sized businesses.

Since the transfer of personal data is otherwise proposed to meet strict requirements, the government can meet its sovereign objectives (for eg. security of citizen's data) without having to mandate any local storage requirements.

Pakistan should consider diplomatic channels, such as signing a Mutual Legal Assistance Treaty with the U.S., and acceding to the Budapest Convention. These steps would create reliable legal channels through which law enforcement officials in Pakistan could request digital evidence. In addition, Pakistan should establish a single point of contact for government-to-government requests. This would ensure that requesting agencies are familiar with U.S. legal and constitutional requirements, and have reviewed requests to ensure they meet U.S. standards. It should also be noted that many U.S. companies have processes for responding to and granting disclosure requests, and that many such requests from Pakistan have been previously granted.

Rationale for removing all data localization measures

a. Most service providers will not already have systems in place that isolate critical personal data from other, general account data. Requiring specialised types of processing for different types of data categories often stored in the same account could actually create privacy risks by requiring companies to sort and identify the data that fall into this category in order to meet these additional requirements.
b. Requiring that certain data only be processed and stored locally would put people and businesses' sensitive or proprietary data at greater risk of a security breach. This is because companies of all sizes use distributed networks, where data storage is spread out over servers in different locations, often in different parts of the world. Distributed networks prove critical to increasing resilience and enabling back-up service in the event of a network failure. Data that is only stored locally would be destroyed or made inaccessible in the event of an outage in that location, significantly hindering the ability of businesses to prosper. Finally, it may be technically impossible for companies offering services on a global scale to comply with the provision in the Draft Bill relating to local storage of data, particularly as it applies to the local processing and storage of "critical personal data".
c. Requiring data to only be stored locally imposes significant data storage costs for companies of all sizes. In addition, such companies will be less likely to invest in state-of-the-art network protection tools. This is because compliance with data localisation regulations requires significant up-front costs for businesses that must purchase and set up the hardware and software that they

rely on. After making that initial outlay of capital, small and medium-sized businesses – and even large companies – are often unable to bear the additional cost to update their data management systems regularly. These costs, and the centralisation of data storage, leave people's data more vulnerable to unauthorised access, exfiltration, and exploitation by malicious actors such as criminal hackers and foreign spies. Where no data localisation mandates exist, technology and tech-dependent businesses can take advantage of cloud storage solutions that allow affordable and scalable ways to deploy the latest technology and tools across the network to make it secure, and that decentralise where sensitive or personal data are stored to ensure it is harder for malicious actors to find and access.

d. Data localisation is not always an effective means of protecting the privacy of individuals or addressing challenges faced by domestic law enforcement in accessing digital evidence of crimes. The data localisation provisions, contrary to the bill's intended purpose of protecting the privacy of individuals, creates a 'honey pot of data' making the data more susceptible to security breaches and cyber attacks. Strict restrictions on the cross-border processing and/or storage of data are not the best way to protect people's privacy and they often introduce significant security risks , and they limit the ability for native tech and tech-dependent industries to grow.
e. Requirements to store data locally are not necessarily effective at protecting people's privacy, and can undermine data security. For example, the U.S. Federal Trade Commission and the European Commission have publicly warned against data localisation as a method for providing privacy protections to users, and have found that a much more effective way to promote robust privacy practices is through laws or regulations that place reasonable limitations on the collection and use of personal data and provide mechanisms that ensure company accountability towards the user.
f. Finally, requiring user data to be stored in-country would not facilitate law enforcement access to data that is held by companies that are based in the United States since they are subject to U.S. law, which places strict limits on their ability to disclose contents and most metadata, subject to certain limited exceptions. The location of where data is stored would not resolve the conflict of law that prohibits U.S. companies from responding to direct requests for contents from Pakistani officials. As the U.S. Justice Department has advised, "data location is often not a good basis upon which to ground requests to produce electronic data." In addition, the U.S. Department of Treasury has found that forced data localisation may "increase cybersecurity and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information."

Given the comments and rationale above, we therefore recommend the following:

- Deleting the requirement that all Critical Personal Data and "some components" of sensitive personal data must be stored locally. In addition to the importance of facilitating cross-border data flows, data localisation harms data security, stifles economic growth, and is not efficacious at addressing concerns related to privacy and law enforcement access to data. As flagged above, such data localisation requirements are more likely to increase costs to businesses seeking to do business internationally (both Pakistan businesses seeking to expand globally and international businesses seeking to target the Pakistan market), resulting in greater costs and fewer options for local consumers and consequently less overall consumer benefit.
- The concept of "Critical Personal Data" be removed from Section 2(o) and the rest of the Draft Bill. The current definition is vaguely defined in the Draft Bill as it is unclear as to what "unregulated e-commerce transactions" and "any data related to international obligations" encompasses. The separate concept of "Critical Personal Data" is out of step with International Benchmarks and the lack of precise definition creates further confusion as to what data is subject to the data localization requirements in Section 14.2 of the Draft Bill. The definitional ambiguity could result in sweeping exclusions from cross-border data transfers and huge increases in compliance costs to small businesses, particularly those local businesses seeking to expand operations cross-border, who may be caught by the very broadly worded "any data related to international obligations" limb of the definition.
- If the MOITT's concern is that certain state secrets or data pertaining to national security not be transferred overseas, then we recommend that this concern would be better addressed in other more appropriate legislation (i.e. legislation pertaining to state secrets or national security) and that this concept should be removed in its entirety from the Draft Bill.

2. Revising requirements around Sensitive Personal Data (SPD) and deletion of Critical Personal Data (CPD) (Sections 2, 14, 15, 29 and 31)

The creation of distinct or special-care categories of personal data (i.e., SPD and CPD) and the corresponding grounds for processing such data should be clearly scoped and based on comprehensive risk assessment. Over-broad special-care categories of personal data can lead to requirements that are over-prescriptive, increasing costs of compliance, adding friction to digital trade, and adversely impacting ease of doing business. It is also our conclusion that the current definitions do not serve to increase privacy protections for individuals and are unfortunately not interoperable with International Benchmarks. Keeping these broad principles in mind, we recommend the following alternative approaches for defining and processing these special-care categories:

a. Exclude "access control data," "financial information," "pictorial or graphical still and motion forms," and "IP address and online identifier," and date related to computerized national identity card and passports from the scope of SPD. Their inclusion makes the category extensive and therefore impractical for business to manage. But more so it serves to decrease the special attention that we believe it is intended should be given to such data. Instead, increase the list of grounds for the processing of such data, in line with international best practices. Article 29.1(a) of the Draft 2021 Bill requires both explicit consent and fulfilment of further conditions before SPD can be processed. While we recognize the Government's objective of ensuring that SPD is subject to a higher standard of care, including: (1) "access control data" (e.g., usernames, passwords); (2) "financial information" (e.g., bank account details, credit, debit card, etc.); (3) "pictorial or graphical still and motion forms;" (4) "IP address and online identifiers;" and (5) "physical identifiable location in the definition of SPD renders the scope of this definition unduly broad. Because of the stricter requirements applicable to SPD, this unduly broad definition creates disproportionate restrictions compared to the potential risk of harm (explained further below), without clear data protection gains for individuals in Pakistan.

   For example, requiring explicit consent for processing of these five categories of data is, in many circumstances, operationally impractical. For example, when a customer wishes to purchase an item, and the cashier needs to process credit card information to complete payment, it is not practicable to require the cashier to ensure that the customer signs an additional form stating that the customer explicitly consents to processing of their payment data for the purpose of the sale and purchase of the item. By handing over a credit card for payment, the customer usually impliedly consents to processing of the credit card information for the purpose of sale and purchase of the item. Requiring explicit consent would adversely impact ease of doing business and would inhibit many ordinary uses of such data – including where processing would clearly benefit the data subject, where the privacy risks are limited, where the data subject could reasonably expect that their data would be processed for a purpose, where written consent cannot be obtained, and where data subjects likely would not object to the processing (e.g., authenticating users of a service, or processing previously-agreed recurring payments).

   For these reasons, data protection laws that have been passed internationally do not typically include additional provisions on the processing of such categories of data. For example, under the European Union's General Data Protection Regulations (GDPR), Financial Information, Access Control Data, IP Addresses, and Cookie Data could be considered personal data if they could

identify an individual but not sensitive data. This is an important distinction as on their own, these data types are not necessarily sensitive. If the Draft 2021 Bill deviates from such international norms, it would ultimately impede innovation and economic development in Pakistan, as foreign corporations which are considering investing or have already invested in Pakistan would likely migrate to other countries with more interoperable personal data protection regimes. For the Draft 2021 Bill to be truly interoperable on a global level, its definitions for SPD must align with existing global frameworks and place a similar gradation of obligations on each type of data. We therefore recommend that "access control data," "financial information," "pictorial or graphical still and motion forms," "IP address and online identifiers", "physically identifiable location" should be excluded from the definition of SPD.

In addition to requiring explicit consent, the Draft 2021 Bill sets out a restrictive set of additional conditions for processing SPD, which also fall outside of international norms. We continue to recommend that: (1) Section 29.1 should be revised to allow for processing of SPD on the basis of either: (i) the data subject's consent; or (ii) the satisfaction of any of the conditions in Section 29.1(b); and (2) the conditions in Section 29.1(b) should be expanded to allow for processing of SPD for any of the following reasons: (i) processing is for employment, social security, and social protection requirements; (ii) processing is necessary for the public interest; (iii) processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes; (iv) processing is carried out by a foundation, association, or any other not-for-profit body with a political, philosophical, religious, or trade union aim in the course of legitimate activities with appropriate safeguards.

b. Delete the category of CPD in its entirety. The Draft 2021 Bill continues to create a special-care category under the label "Critical Personal Data" and imposes additional obligations on entities that engage in the processing of such data, including preventing transfers of such data across borders (Section 14.2). The objective behind inclusion of this special-care category is unclear, and the provided types of data that would constitute CPD are ambiguous and problematic - data relating to, "public service providers", "unregulated e-commerce transactions" and "international obligations". No definitions or criteria for data relating to "unregulated e-commerce transactions" or "internal obligations" have been provided in the Draft 2021 Bill and the definition of "public service provide" is overbroad and vague. In light of the above, organizations will certainly face operational difficulties in complying with the Draft 2021 Bill, as organizations would not be able to determine with any

reasonable certainty what types of data should be treated as CPD and stored in-country. This ambiguity around the definition and scope of CPD will increase compliance and service costs and will limit innovation for companies in Pakistan, with the greatest impact on small to medium business and start-ups. The inclusion of CPD as a special-care category also does not enhance privacy protection. We therefore recommend that: (1) the category of CPD; and (2) the obligations arising from processing of CPD should be deleted from the Draft 2021 Bill entirely.

Given the comments and recommendations above, we propose the following amendments to the drafting language.

2. Definitions

d) "Authority" means the Personal Data Protection Authority (PDPA) established under section [32] of the Act~~; "Critical Personal Data" – to be classified by the Authority with the approval of the Federal Government~~.

14. Cross border transfer of personal data *(…)*

~~14.1 Critical personal data shall only be processed in a server or data centre located in Pakistan.~~

~~14.2 Notwithstanding anything contained in sub-section (1), the Federal Government may notify certain categories of personal data as exempt from the requirement under sub-section (1) on the grounds of necessity or strategic interests of the State.~~

~~14.3 Nothing contained in sub-section (3) shall apply to sensitive personal data.~~

15. Framework on conditions for Cross border transfer of personal data *(…)*

~~15.2 The Authority shall also devise a mechanism for keeping a copy of personal data in Pakistan to which this act applies.~~

30. Exemption *(…)*

30.2 Subject to section [28] ~~and critical personal data~~,
personal data— (…)

3. **The restrictions around cross-border transfers of data should be clarified and narrowly tailored to achieve their intended policy goals**

The general rule in Section 14.1 of the Draft Bill is that personal data may be transferred outside of Pakistan as long as the destination country offers a data protection "legal regime" that is at least equivalent to that under the Draft Bill.

Data protection laws must facilitate intercompany and cross-border data flows, while protecting individuals. While often well-intentioned, cross-border data transfer restrictions can be damaging to the modern, globalised economy as it increases the barriers to doing business across borders and providing citizens with greater service and product offerings. In line with the OECD Privacy Principles, cross-border data transfers should be permitted as long as the data controller remains accountable for protecting the data regardless of geographic location.

However, we note that the Commission has the power under Sections 15.1 and 34(2)(c) of the Draft Bill to prescribe further conditions that must be adhered to for cross-border data transfers. We wish to flag that the subsequent framework and conditions to be released under these powers should not be unduly prescriptive. We recommend that

Sections 15.1 and 34(2)(c)(xii) be removed to mitigate against unduly restrictive cross-border data transfer requirements that will stifle both the growth of domestic companies abroad as well as the willingness of foreign companies to invest and establish themselves in Pakistan. We further suggest that the Draft Bill explicitly recognises contractual mechanisms ("standard contractual clauses"), intra-group transfer schemes ("binding corporate rules") and certifications, such as the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System ("APEC CBPRS"), as permitted cross-border transfer mechanisms in line with other International Benchmarks including GDPR and Singapore's PDPA. Regional standard-setting privacy regimes, such as Japan's Act on the Protection of Personal Information, enable data controllers to also transfer data on the basis of consent, in addition to the permitted transfer mechanisms outlined above.

We further recommend that exceptions to the requirement in Section 14.1 be introduced in line with International Benchmarks such as Article 49 GDPR to accommodate situations where, for example, such transfers are necessary for the vital interests of the data subject or for the public interest, amongst others.

We recommend the following amendments to Section 14 and 15:

14. Cross border transfer of personal data *(…)*

~~*14.1*~~ *Provided that if personal data is required to be transferred to any system located beyond territories of Pakistan or system that is not under the direct control of any of the governments in Pakistan, it shall be ensured that the country where the data is being transferred offers personal data protection at least equivalent to the protection provided under this Act and the data so transferred shall be processed in accordance with this Act* ~~*and, where applicable, the consent given by the data subject*~~.

~~*14.1*~~ *The requirements under sub-section (1) shall not*

apply where:

a) the transfer is necessary for:

(i) the protection of the vital interests of the data subject;

(ii) important reasons of public interest;

(iii) the establishment, exercise or defence of legal claims; or

b) the data subject has consented to the transfer to that recipient or class of recipients outside Pakistan.

15. Framework on conditions for Cross border transfer of personal data *(…)*

~~*15.1 Personal data other than those categorize as critical personal data may be transferred outside the territory of Pakistan under a framework (on conditions) to be devised by the Authority.*~~

~~*15.2 The Authority shall also devise a mechanism for keeping a copy of personal data in Pakistan to which this act applies.*~~

15.1 The data controller shall be deemed to have fulfilled its obligation under section 14 to ensure that the country where the data is being transferred offers personal data protection at least equivalent to the protection provided under this Act where:

a) the data controller enters into a legally binding and enforceable instrument with the recipient located outside Pakistan which obligates the recipient to

protect the personal data so transferred to a standard at least equivalent to the protection under this Act;

b) the transfer is made to a recipient which controls, is controlled by or is under common control with the data controller, and pursuant to a set of binding corporate rules applicable to both the data controller and such recipient which obligates the recipient to protect the personal data so transferred to a standard at least equivalent to the protection under this Act;

c) the transfer is pursuant to a code of conduct approved by the Authority with binding and enforceable commitments of the recipient outside of Pakistan to apply appropriate safeguards, including as regards to data subjects' rights; or

d) the transfer is pursuant to any other instrument, treaty or international certification recognized by the Authority which permits the transfer of Personal Data from Pakistan to the country in which the recipient is located.

4. **The extraterritorial application of the Draft Bill in Section 3 should either be deleted or aligned with Article 3 GDPR and other International Benchmarks, and the overall drafting of that section should be clarified**

Section 3 of the Draft Bill states that it applies to: (A) all persons that process, have control over, or authorise the processing of personal data, where the data controller or data processor is located in Pakistan, (B) all foreign-incorporated data controllers or data processors who operate (whether "digitally or non-digitally") in Pakistan and are involved in any commercial or non-commercial activity in Pakistan, (C) all processing outside of Pakistan in places where Pakistani law applies "by virtue of private and public international law", and (D) any data subject in Pakistan. This is substantially broader than the April 2020 draft of the Bill which focused on processing with a nexus in Pakistan (the data controller, data processor or data subject had to be located in Pakistan).

This extra-territoriality is also wider than that under Article 3 of GDPR, which only applies to controllers or processors located outside of the EU 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). The thresholds in this version of the Draft Bill are much wider than those under GDPR, including foreign entities engaged in the broadly worded "non-commercial" activity in Pakistan, and foreign entities to whom Pakistani laws apply "by virtue of private and public international law". This vague drafting could effectively include within the purview of the Draft Bill foreign entities that may not be processing any personal data from Pakistan, or even in Pakistan,

but who are doing so pursuant to a commercial agreement which has Pakistan law as its governing law.

A clearly defined jurisdictional scope is important for both organisations and data subjects who seek to understand and manage their privacy obligations and rights. The expanded scope described above 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, and may also cause international organisations to be more resistant to choosing Pakistani law as the governing law of their contracts. This would clearly result in fewer benefits and choices to individuals and companies in Pakistan and we therefore recommended that this extraterritorial scope in Section 3 be deleted.

If despite these concerns the extra-territoriality is retained, we recommend aligning the provision with the position under GDPR (including the clarifications in Recital 23 of GDPR regarding what constitutes the offering of goods and services), to include minimum thresholds regarding the processing of Pakistan-based data subjects' personal data.

We recommend the following amendments to Section 3:

3. Scope and applicability

3.1. This Act applies to:
a) any data controller or processor established in Pakistan, who is involved in the processing of personal data, regardless of whether the processing takes place in Pakistan or not; and

b) any data controller or processor not established in Pakistan, who is involved in the processing of personal data of data subjects located in Pakistan, where the processing activities are related to:

(i) the offering of goods or services to data subjects in Pakistan, irrespective of whether payment by such data subjects is required; or
(ii) activities within Pakistan of such data subjects.

~~*a) any person who processes; or*~~

~~*has control over or authorizes the processing of, any personal data provided*~~ ~~*any of the data subject, controller, or processor (either local or foreign) is*~~ ~~*located in Pakistan.; Subject to subsection (1),This Act applies to a person in*~~ ~~*respect of personal data if*~~

3.3 For the purposes of ~~subsections (2) and (3)~~ sub-sections (1) and (2), each of the following is to be treated as established in Pakistan:

a) an individual whose physical presence in Pakistan shall not be less than one hundred and eighty days in one calendar year;
b) a body incorporated under the Companies Act 2017 (Act XIX of 2017);
c) a partnership or other unincorporated association formed under any written laws in Pakistan; and
d) any person who does not fall within paragraph (a), (b) or (c) but maintains in Pakistan—
(i) an office, branch or agency through which he carries on any activity; or
(ii) a regular practice.

3.4 For the purposes of determining whether a data controller or processor is offering goods or services to data subjects in Pakistan under clause (b)(i) of sub-section 1, the mere accessibility of the data controller's or processor's or an intermediary's website in Pakistan alone shall not be sufficient to ascertain such intention, and the following non-exhaustive factors shall also be taken into account:

a) the use of Urdu or the display of prices in Pakistani rupees with the possibility of ordering goods; or
b) the express targeting of customers or users who are in Pakistan.

5. The requirements relating to the processing of personal data under Chapter II of the Draft Bill should be aligned with International Benchmarks and should seek to uphold privacy rights of individuals without unduly stifling innovation and business, or undermining privacy or data security.

a. The requirement to protect and secure personal data should be proportionate to the sensitivity and nature of the personal data in question.

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. We therefore recommend deleting the requirement in Section 8.1 of the Draft Bill that data controllers and data processors comply with specific security standards which will be prescribed by the Commission.

Prescriptive security standards are arbitrary, increase compliance costs for organisations, and may not always result in tangible benefits for the data subject. 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.

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. We note that the Draft Bill already mandates in Section 8.2 that the security measures to be implemented must take into account several factors including the nature or harm that may result from the loss or misuse of the personal data. This requirement in itself would be sufficient and is reflective of International Benchmarks.

We therefore recommend that the following changes be made to Section 8 of the Draft Bill:

8. Security requirements

~~*8.1 The Authority shall prescribe standards to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.*~~

8.1~~2~~ A data controller or processor shall, when collecting or processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction ~~in the terms mentioned under sub-section (1)~~ by having regard—

a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction;

b) to the place or location where the personal data is stored;

c) to any security measures incorporated into any equipment in which the personal data is stored;

d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and

e) to the measures taken for ensuring the secure transfer of the personal data.

8.2~~3~~ Where processing of personal data is carried out by a data processor on behalf of the data controller, the data controller shall, for the purpose of protecting the personal data in the terms mentioned at sub-section (1) ensure that

the data processor undertakes to adopt ~~applicable~~appropriate technical and organisational security standards governing processing of personal data~~, as prescribed by the Authority~~.

b. *Flexibility should be built into the requirement to delete and destroy personal data in Section 9 of the Draft Bill, and further exceptions to address situations where personal data must be retained for legal and/or audit purposes should be included.*

Section 9.1 of the Draft Bill states that personal data should not be retained longer than is necessary for the fulfilment of the purpose it was collected for or as otherwise required by law.

We recommend that additional provisions be included to provide organizations 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 Draft Bill should also provide enough flexibility to this requirement 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 the above, inspiration can be taken from Singapore's Personal Data Protection Act, which permits organisations to retain personal data where it is necessary for any legal or business purposes. We suggest also including "operational" purposes in this Draft Bill to reflect the technical limitations outlined above.

We suggest that the following changes be made to Section 9:

9. Data retention requirements 9.1 *The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose or for legal, operational or business purposes.* *9.2 It shall be the duty of a data controller to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed or for legal, operational or business purposes.*

c. *The prohibition in Section 12 of the Draft Bill on transferring data to an "unauthorised person or system" should be deleted.*

There is a general prohibition in Section 12.1 on personal data being transferred to "any unauthorised person or system and contrary to the provisions of the Act". However, it is unclear what amounts to an "unauthorised person or system". This prohibition further creates confusion in relation to the other requirements in Sections 5 and 7 of the Draft Bill relating to the processing and disclosure of personal data.

Section 5 of the Draft Bill already sets out the general situations under which personal data may be processed, while Section 7 provides that the data controller may only disclose personal data without requiring further consent: (a) for the purposes disclosed to the data subject; or (b) for purposes directly related to the disclosed purpose; or (c) to those classes of third parties specified in the notice given to the data subject.

When read together with Section 12.1, confusion may arise where a data subject has already consented to a disclosure to a particular person or system, but that person or system is deemed as "unauthorised" under Section 12.1. We therefore recommend that Section 12.1 be deleted in its entirety.

d. *The requirement in Section 5.1 of the Draft Bill that separate consent be obtained by a data controller for each purpose of processing should be deleted as it is unduly burdensome for both consumers and businesses and out of step with International Benchmarks.*

The latest version of the Draft Bill introduces a requirement in Section 5.1 that separate consent must be obtained from the data subject for each purpose of processing. This is overly prescriptive and may result in prohibitively high costs for local Pakistani businesses and decrease, rather than increase privacy protection for consumers. Furthermore, the notice requirement already provides sufficient safeguards for transparency where consent is relied on as the lawful basis of processing.

Notice and consent obligations are important features of any privacy law framework as they contribute to greater transparency and understanding amongst data subjects of how their data is being processed. However, privacy laws should not prescribe in detail the way consent must be obtained because the type of consent that is appropriate will depend on the context. Flexible consent requirements ensure that organizations do not have to spend undue resources seeking consent to use personal data whilst ensuring, individual privacy will still be protected through other requirements.

International Benchmarks typically require new, separate consents for ***new*** purposes that were not previously notified to the data subject. This approach balances individual privacy rights against the administrative burden involved in seeking consent from consumers. Requiring separate consents for each purpose notified to consumers at the outset would result in notice and consent fatigue in consumers who, for example,

would have to provide consent five separate times to a single privacy notice that contains five different purposes of processing. The separate consents do not provide any additional benefit to consumers, and instead increase operating costs for small businesses who will have to ensure that their consent mechanisms are unduly granular. Local consumers may also be less willing to provide consent where it is unduly cumbersome, which would limit the number of innovative services that they can enjoy.

Prescriptive consent obligations are burdensome, difficult, impractical, and costly to implement. They ultimately will disincentivize Pakistani companies from data innovation and hinder the development of Pakistan's digital economy. We therefore recommend that this requirement for separate consents be removed from Section 5.1 of the Draft Bill.

6. The data subject rights in Sections 25 and 26 of the Draft Bill should be deleted as they are not consistent with general privacy principles and the International Benchmarks, the timeline for complying with an exercise of the right in Section 27 should have more flexibility, and the new "General Protected Rights" in Section 28 should either be deleted or aligned with the International Benchmarks.

a. *The right to cease processing due to unwarranted and substantial damage or distress in Section 25 should be deleted.*

There is no clarity as to what "unwarranted" and "substantial damage or distress" entails, which may result in multiple baseless requests to cease processing personal data on this ground. The fact that this damage or distress may be to a person other than the data subject also broadens this right substantially and creates an administrative burden on businesses of all sizes that must respond to these requests. The Draft Bill already provides a range of, user rights, such as right of erasure, and/or withdrawing consent, which would ensure a high level of user control over their data in line with accepted international benchmarks.

b. *The right for foreign data subjects provided in Section 26 should be deleted.*

The intent of the provision is unclear and we respectfully request greater clarity on the motivations for including this as we consider that there may be other ways of addressing the issues that MOITT seeks to remedy that are more aligned with International Benchmarks and best practice. While MOITT has, in the this latest Draft Bill, included a new definition of "foreign data subject" as being "a data subject who is not a Pakistani national", this does not add any further clarity to Section 26. As currently drafted, the right creates uncertainty in respect of the obligations data controllers in Pakistan would have to comply with, as it imposes obligations arising under the laws of other jurisdictions as well.

c. *There should be more flexibility built into the timeframe for complying with a data subject request to erase personal data in Section 27.1 of the Draft Bill.*

The data controller has an obligation under Section 27.1 of the Draft 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, GDPR Article 12 affords data controllers one month to respond to a request and this can be extended by a further two months.

We propose the following amendments to Section 27.1 of the Draft Bill:

> ***27 Right to erasure***
>
> 27.1 The data subject shall have the right to obtain from the data controller the erasure of personal data concerning him as soon as reasonably possible ~~without undue delay~~ and the data controller shall have the obligation to promptly erase personal data ~~within a period of 14 days~~ where one or more of the following condition applies:

d. *The new "General Protected Rights" under Section 28 should be removed or expanded upon in line with International Benchmarks*

The new Section 28 of the Draft Bill seeks to introduce a new data portability right and a new right not to be subject to a decision based solely on automated processing, including profiling. While these rights are generally aligned with those data subject rights found in International Benchmarks, the drafting in the Draft Bill lacks the necessary specifics that would make it clear for organisations to help give effect to these rights.

For example, there is no clarity on what the right to data portability entails and how the data subject's rights in this regard will be protected. Similarly, it is unclear if the right not to be subject to decisions based solely on automated processing means that there is a blanket prohibition on such processing or if data subjects must, for example, provide express opt-in consent to such processing. Such confusion and lack of clarity would hinder rather than help efforts to strengthen the rights of data subjects since there are no concrete details to guide the implementation of these rights.

If MOITT wishes to retain these rights, we recommend that further drafting be included to align the rights with those under International Benchmarks. For example, Article 20 GDPR can be used as a reference for the implementation of the data portability right, whilst Article 22 GDPR can be referred to in relation to the automated processing right.

We propose the following amendments to Section 28 of the Draft Bill:

28. ~~*GENERAL PROTECTED RIGHTS*~~ ***RIGHT TO DATA PORTABILITY***

~~*Not contrary to any other law, the following rights of the data subject are protected under the Act.*~~

~~*a. Right to Data Portability*~~

~~*b. Right not to be subject to a decision based solely on automated processing, including profiling.*~~

28.1 The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data controller without hindrance from the data controller to which the personal data have been provided, where:

a) the processing is based on consent pursuant to sub-section (1) of section 5 or sub-section (1)(a) of section 29 or on a contract pursuant to sub-section (2)(a) of Section 5; and

b) the processing is carried out by automated means.

28.2 In exercising his or her right to data portability pursuant to sub-section (1), the data subject shall have the right to have the personal data transmitted directly from one data controller to another, where technically feasible.

28.3 The exercise of the right referred to in sub-section (1) shall be without prejudice to Section 27. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

7. Improve the clear assignment of responsibility between data controllers and data processors for data breach notification (Section 13)

It is vitally important that data protection frameworks clearly outline the respective responsibilities of data controllers and data processors. This will ensure that all parties

which are subject to the data protection law understand what they are responsible for. The Draft 2021 Bill broadly achieves this by clearly stating that the Data Controller is the main entity that is responsible for compliance with the data protection law.

However, we note that Section 13 of the Draft 2021 Bill inappropriately requires Data Processors to issue personal data breach notifications if they "become aware" of a personal data breach. This provision overlooks the fact that data processors are engaged by data controllers to process data (typically through a contractual relationship) and therefore, only process data *on behalf of* such data controllers. Because of this, the processor may not have the necessary control over the data, may not know that it is processing personal data, or may be unable to accurately furnish information required under the reporting mechanism proposed in the Bill. Additionally, requiring both the controller and the processor to report breaches could result in erroneous or conflicting reporting of a breach, which could in turn create confusion for the Authority as to the nature of the breach.

In order to streamline this process, we repeat our previous recommendation that Section 13.5 be amended to require data processors to report a personal data breach *only to the data controller* upon becoming aware of a breach. This does not prevent data processors from informing data controllers about data breaches they become aware of in the duration of the contract. The sole and ultimate responsibility for notifying the Authority and/or affected data subjects of such a breach must lie with the data controller.

8. **The conditions for processing sensitive personal data should be clarified and the definition of "sensitive personal data" should be aligned with the concept of "special categories of personal data" under GDPR.**

We understand that MOITT previously had plans to remove "access control data" from the definition of "sensitive personal data" in Section 2(t) of the Draft Bill, which we supported. However, this has not been removed in the latest Draft Bill and we urge MOITT to reconsider this. Sensitive personal data is usually given a higher level of protection because it is more sensitive. The definition of "sensitive personal data" should therefore only include information that is by nature of a higher risk to individual privacy, and not information such as IP addresses, online identifiers, usernames and passwords that may not in some cases even be able to identify an individual. We also recommend that the reference to "financial information" be removed from the definition of "sensitive personal data" for this reason. Not all types of financial information are always at higher risk to individual privacy and so a blanket inclusion of "financial information" 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, we understand that financial information 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 therefore such data should not also be separate sensitive personal data requirements under this Draft Bill for consistency.

As currently drafted, the requirements of Section 29 are also subject to Section 5.2, which provides for a number of other legal bases for the processing of personal data. For greater clarity and since the requirements under Section 29.1 are more specific than those in Section 5.2, we suggest that the words "Subject to" at the start of Section 29.1 be amended to read "Notwithstanding" to make it clearer that when processing sensitive personal data, only the requirements of Section 29 need to be complied with, and that the requirements under Section 5.2 only apply to the processing of non-sensitive personal data.

We recommend the following amendments to Sections 2 and 29:

2. Definitions

In this Act, unless there is anything repugnant in the subject or context,— (…)
*(k) "**sensitive personal data**" means ~~and includes~~ data relating to ~~access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, and,~~ passports, biometric data, and physical, psychological, and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, or any other information for the purposes of this Act and rules made thereunder.*

29. Processing of sensitive personal data

29.1 ~~Subject to~~ Notwithstanding subsection (2) of section 5, a data controller shall not process any sensitive personal data of a data subject except in accordance with the following conditions:

a) the data subject has given his explicit consent to the processing of the personal data; ~~and~~ or
b) the processing is necessary— (…)

9. **Expansive powers and insufficient guardrails for the Commission (Sections 15 and 34).**

   a. **The Commission should not be responsible for creating frameworks on behalf of law enforcement or national security agencies.** We are deeply concerned about newly-included requirements that "some components" of SPD should be retained in Pakistan for public order or national security purposes (Section 15.2). As the Draft 2021 Bill currently stands, the phrase "some components" is completely undefined. In addition, it does not specify how or what criteria/thresholds will be used to designate the components of sensitive personal data as being 'related to public order or national security. This can lead to unreasonable and arbitrary classifications and distinctions with respect to the treatment of personal data under law. This ambiguity would create significant regulatory uncertainty and **undue compliance burdens** for citizens and businesses to comply with the law.

   While we recognize that law enforcement agencies have legitimate needs to be able to request and access personal data (e.g., for national security or investigating criminal activity), law enforcement agencies already have existing powers and processes to obtain these types of data. Hence, the inclusion of this provision in the Draft 2021 Bill is unnecessary. It is wholly inadequate for a Data Protection Commission (Commission) to be the party responsible for devising a mechanism or framework for defining the types of data to be retained in the country.

   The independence of the Commission is vitally important in data protection frameworks as this ensures that citizens trust that the Commission will protect consumer interests. The Commission's role should therefore be to ensure that the needs of law enforcement or national security agencies are appropriately balanced against privacy and data protection objectives, rather than to create a framework for law enforcement or national security to access or retain data. **We therefore recommend that Section 15.2 should be deleted from the Draft 2021 Bill entirely.**

   b. **The Commission should not have broad power and discretion to create entirely separate regulatory frameworks that are not clearly outlined in the main Data Protection Act.** We are deeply concerned about the broad and unfiltered discretionary powers provided to the Commission under Section 34 of the Draft 2021 Bill. In particular, Section 34(2)(d) provides the Commission with the power to "*identify big / large data controllers / processors, along with other categories*" and "*define special measures for compliance.*" This would

seemingly permit the Commission to create *ex-ante* regulatory frameworks on such companies and could subject them to arbitrary requirements over and above those obligations already outlined in the Data Protection Act, even if the company has not breached any requirement under the Data Protection Act. This power is too broad and lacks appropriate safeguards, such as public consultation and measures to ensure that the companies subject to the Data Protection Act agree to any additional measures.

Singling out certain categories of companies, based on size or another such subjective measure rather than whether the company is in breach of the data protection law, is inconsistent with modern data protection laws and unprecedented globally. International best practice is to apply and differentiate legal requirements based on the data being collected, rather than the company collecting the data. If Pakistan were to move forward with this proposal, it would create significant regulatory uncertainty for corporations, dampen the attractiveness of Pakistan as a destination for foreign direct investment, and stymie the growth of Pakistan's digital economy. **We therefore recommend that: (1) Section 34(2)(d) should be deleted from the Draft 2021 Bill; and (2) appropriate guardrails should be introduced for the general powers ascribed to the Commission under Section 34, including a commitment for the Commission to consult publicly prior to issuing any compliance frameworks or guidelines**.

10. The Draft Bill should expressly state whether a DPO must be appointed, and if so, include more details on the qualifications and requirements of such a DPO.

Data protection officers ("DPOs"), play an important role in ensuring an organisation complies with privacy laws and facilitating the exercise of data subject rights. However, it is unclear from the Draft Bill if data controllers and processors will be required to appoint a DPO. There is some mention in Section 34(2) that the Commission may formulate further rules in relation to the "responsibilities of Data Protection Officers", and Section 13.3 requires data controllers to include the name and contact details of the data protection officer in a personal data breach notification. However, there is no express obligation to appoint a DPO in the Draft Bill.

If a DPO must be appointed, we recommend that this be expressly set out. We also recommend that sufficient flexibility be given to organisations to appoint their DPO. Internationally, best practice in this area provides for flexibility in allowing organisations to choose who acts as the DPO. This enables organisations to appoint an individual or group of individuals who will act as the DPO in a way that best reflects the organisation's structures and processes. For example, smaller organisations may

only wish to appoint one individual as its DPO due to the size and scale of the business. Multinational organisations, however, may wish to appoint a centralised team as its DPO that oversees privacy across multiple markets due to the scale of the organisation and their processing of personal data.

Most large entities have centralised and streamlined processes for handling queries in relation to the processing of any personal data. These processes are generally overseen by a Data Protection Officer who need not be located in a specified jurisdiction. Instead the Data Protection Officer will be required to respond to reasonable requests as per applicable legislation in a timely manner. If the office and such requirements are meant to be localised in each and every jurisdiction that global service providers operate in this would be infeasible and cost prohibitive, deterring such organisations from targeting and offering their products and services in Pakistan.

We recommend that following be added as a new section in the Draft Bill at the end of Chapter I:

3A. Data Protection Officer

3A.1 A data controller or processor falling within sub-section (1)(a) of section 3 shall appoint a data protection officer, being an individual or group of individuals, whether located within or outside Pakistan to be responsible for ensuring that it complies with this Act.

3A.3 The designation of a data protection officer under sub-section (1) shall not relieve the data controller or processor of any of its obligations under this Act and such data controller or processor shall remain responsible for ensuring its own compliance with this Act.

11. The Draft Bill's criminal penalties and fines should be deleted

While we note that several criminal fines and sanctions have been removed since the 2018 draft of the Bill and imprisonment has been removed as a possible penalty in Section 23, criminal liability for any breach of the processing and disclosure requirements is still imposed in Section 44 of the Draft Bill (as well as in Sections 23 and 47), while the quantum of fines remains high in Sections 23, 44, 45, 46 and 47 as well. The new provisions in Section 46 that permit the Commission to impose a fine of up to 250 million rupees for a failure to respond to a notice from the Commission for reasons as to why an enforcement order should not be issued, a failure to adequately explain an alleged contravention to the Commission, and to remedy an alleged contravention of the Act within the timeline prescribed by the Commission are also

very high, particularly in light of the fact that contraventions of an enforcement order themselves only result in a fine of up to 2.5 million rupees under Section 46. These clauses are contradictory and confusing and should therefore be deleted.

Section 47 of the Draft Bill still mandates that where any breach is committed by a legal person, the maximum fine that may be imposed is the higher of 1% of its gross revenue in Pakistan or 30 million rupees, and the individuals responsible may also be personally liable.

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 privacy law, 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 as a last resort.

Criminal penalties are not an appropriate remedy for most violations of privacy laws. A regulatory regime that relies on criminal fines and other criminal sanctions hinders collaboration between regulators and organisations and ignores opportunities to adopt other means to prevent harm. Remedies and penalties for a breach of privacy obligations should be graduated and proportionate to the harm resulting from that breach. A tiered approach to sanctions is therefore generally considered best practice, with warnings, administrative fines and other clearly structured civil measures all proving effective in fostering compliance. This allows for a more collaborative and open relationship between the Regulator and organisations as it incentivises communication between them and maximises voluntary compliance.

In addition, best practice internationally points to not drawing any distinction in privacy laws between the types of sanctions that apply to different types of businesses (e.g. whether it is a large multinational corporation or a sole proprietorship). Individual privacy rights should not depend on how a service provider or vendor has legally structured their business. We therefore recommend that the separate sanctions on "legal persons" or corporate entities be deleted in Section 44. We understand that some clarity is needed on whether any individuals acting on behalf of a corporate entity will be liable for the entity's breach. We propose that similar wording to that in the Singapore PDPA be adopted, clarifying that such individuals will only be liable where it can be demonstrated that the breach of the Act was caused by the relevant individual.

We propose the following changes to Sections 23, 44 and 47 of the Draft Bill:

23. Withdrawal of consent to process personal data *(…)*

23.4 A data controller who contravenes subsection (2) ~~commits an offence and~~ shall~~, on conviction,~~ be liable to a fine not exceeding five million rupees ~~or to imprisonment for a term not exceeding one year or to both~~.

44. Unlawful processing of personal data *(…)*

44.1 Anyone who processes or cause to be processed, disseminates or discloses personal data in violation of any of the provisions of this Act shall be punished with a fine up to fifteen million rupees and in case of a subsequent unlawful processing of personal data, the fine may be raised up to twenty five million.

44.2 ~~In case the offence committed under sub-section (1) relates to sensitive data the offender~~ Anyone who processes or cause to be processed, disseminates or discloses sensitive personal data in violation of any of the provisions of this Act may be punished with a fine up to twenty five million rupees.

47. Corporate liability

47.1 Where a breach of this Act committed by a legal person is proved —

(a) to have been committed with the consent or connivance of an officer, member or other person with authority to take decisions on behalf of that legal person; or

(b) to be attributable to any neglect on his part,
the officer as well as the legal person shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

~~A legal person shall be held liable for a non-compliance committed on his instructions or for his benefit or lack of required supervision by any individual, acting either individually or as part of a group of persons, who has a leading position within it, based on a power of representation of the person; an authority to take decisions on behalf of the person; or an authority to exercise control within it. The legal person shall be punished with fine not exceeding 1% of its annual gross revenue in Pakistan or thirty million rupees, whichever is higher.~~

~~Provided that such punishment shall not absolve the liability of the individual, who has committed the offence.~~