SUBMISSION ON THE PAKISTAN PERSONAL DATA PROTECTION BILL 2020

1. PART 1: COVER LETTER

11 November 2020

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

Subject: Asia Internet Coalition (AIC) Submission on Pakistan's Data Protection Bill 2020 (Industry Submission following the meeting with MoITT on 14 October 2020)

Dear Minister Syed Amin Ul Haque,

On behalf of the Asia Internet Coalition ("AIC") and its members, I am respectfully submitting our recommendations regarding the Pakistan Personal Data Protection Bill that was published on 9 April 2020 (the "**Draft Bill**"). This is a follow-up to our original submission, dated 15 June 2020.

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. We recognize the on-going efforts of the Ministry of Information Technology and Telecommunications ("**MOITT**") in further fine-tuning the draft legislation since its initial release in July 2018, so as to work towards implementing a comprehensive framework for the protection of personal data in Pakistan.

However, in its current form, this draft presents significant interoperability issues and falls short of international best practices. It will adversely impact Pakistan's digital ambitions and make it difficult for foreign companies to operate and offer services to Pakistani businesses and users.

We encourage MOITT to make a revised version of the Bill available for further public consultation so that we can provide additional recommendations based on international best practices. 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 therefore request the opportunity to engage in further consultations with MOITT based on an improved Draft Bill.

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**").

In Part 2 of this letter, we reiterate our key concerns and recommendations in respect of the Draft Bill. Furthermore, in response to your request during our recent meeting, we have provided specific suggested edits to the text of the Draft Bill. 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. We have structured these comments in order of suggested priority.

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 (MoITT)
- Mr. Syed Faisal Ali Subzwari, Convenor of Advisory Council for the Ministry of Information Technology and Telecommunication (MoITT)
- Mr. Eazaz Aslam Dar, Additional Secretary, Ministry of Information Technology and Telecommunication (MoITT)
- Mr. Syed Junaid Imam, Member IT, Ministry of Information Technology and Telecommunication (MoITT)
- Major General (R) Amir Azeem Bajwa, Chairman, Pakistan Telecommunication Authority (PTA)
- Mr. Syed Ali Abbas Hasani, Managing Director (Acting), Pakistan Software Export Board (PSEB)

2. PART 2: COMMENTS AND RECOMMENDATIONS

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

(i) Key issues and comments

We are highly concerned that the data localisation requirements in the Draft Bill will inadvertently undermine privacy and data security, stifle innovation and growth in technology and internet-dependent industries, while not necessarily addressing the challenges that Pakistan law enforcement faces obtaining digital evidence in criminal investigations. Section 14.1 requires that "Critical Personal Data," a category of data which is not clearly defined, must be processed and stored solely within the borders of Pakistan. Additionally, Section 15.2 requires the Authority to introduce a data localisation framework to force companies to store copies of personal data in Pakistan, even where that data may otherwise be transferred out of the country. We strongly encourage the legislator to reconsider the wording of both provisions so as to remove data localization requirements, which are not consistent with best practices in data protection law.

Requiring that certain data only be processed and stored locally will likely 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". Indeed, the technical infeasibility of complying with such a requirement is a primary reason why many global companies do not offer services in China.

Requiring data to only be stored locally or requiring a copy of data to be stored locally even where it can be transferred and stored elsewhere as well, 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.

Data localisation requirements will also make it harder for Pakistan to harness the value of technology, stifling innovation, economic growth, and IT exports. Companies that provide internet users around the world with innovative and dynamic means of communicating and conducting business do so in reliance on the global free flow of information. It is well-recognised that robust data flows are a significant contributor to the success of modern globalised economies. When governments impose data localisation requirements on businesses that are based or operating within their borders, it stifles their potential for economic growth. This could be especially true for Pakistan, where the IT sector is poised to become the largest export industry in the country, and is a major contributor to the national GDP. For Pakistan to continue to grow its information technology sector in relation to global markets, cross-border data flows are a critical driver which must be encouraged and preserved.

Additionally, requirements to store data locally are not effective at protecting privacy. 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. We recommend that in lieu of introducing restrictive requirements on data storage and transfers, the Draft Bill should hold fiduciaries responsible for implementing sufficient privacy measures to ensure the equal protection of the data that is processed locally and transferred abroad.

Furthermore, 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. This holds true for companies based in the European Union, where legal obligations under the GDPR prevent companies from disclosing personal data to authorities located elsewhere unless certain requirements are met. The location of where data is stored would not resolve this conflict of law. 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."

Pakistan should consider diplomatic channels, such as signing a Mutual Legal Assistance Treaty with relevant jurisdictions, 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 may want to 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, including on the basis of cooperation and that many such requests from Pakistan have been previously granted.

In light of the significant concerns that data localisation requirements raise, we recommend removing the requirement that a copy of all personal data must be stored locally. As noted, data localisation harms data security, stifles economic growth, and does not solve issues of access to digital evidence stored abroad. As flagged above, such data mirroring

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.

We also recommend that the concept of "Critical Personal Data" be removed from Section 2(o) and accordingly from the rest of the Draft Bill. Such data is not clearly defined in the Draft Bill and is meant to be determined by the Authority with the approval of the Federal Government. 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 localisation requirements in Section 14.2 of the Draft Bill. The definitional ambiguity could result in sweeping exclusions from cross-border data transfers and excessive increases in compliance costs to small businesses.

The requirement that this data only be processed in a server or data centre located within Pakistan, unless the Federal Government deems it necessary not to do so or for the "strategic interests of the State", introduces legal uncertainty and is also overly burdensome, if not impracticable in terms of compliance.

If the MOITT's concern is that certain state secrets or data pertaining to national security would be transferred overseas, we recommend that this concern be addressed in other more appropriate legislation (i.e. legislation pertaining to state secrets or national security) and that such matters be removed in their entirety from the Draft Bill.

We also wish to flag that there is a qualification in Section 14.3 that "nothing in sub-section (3) shall apply to sensitive personal data". It is unclear if this is meant to refer to the rule that critical personal data must only be processed in Pakistan or the power of the Federal Government to carve out certain types of data from that requirement. We recommend that this be deleted to achieve greater clarity in the application of the cross-border transfer requirements, which are also discussed further in item 2.2 below.

(ii) Specific drafting recommendations

In light of the above, we recommend that Sections 2, 14, 15 and 30 of the Draft Bill be amended follows:

2. DEFINITIONS

*o) "**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. –

(…)

~~*15.1. 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.*~~

30. EXEMPTION

(…)

30.2 Subject to section [28] ~~*and critical personal data*~~*, personal data—*

(…)

2.2 The restrictions around cross-border transfers of data should be clarified and reframed to achieve their intended policy goals.

(i) Key issues and comments

The general rule in Section 14 Paragraph 1 of the Draft Bill is that personal data may be transferred outside of Pakistan as long as the destination country offers a standard of protection 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. Although often well-intentioned, cross-border data transfer restrictions can be damaging to the modern, globalised economy as they increase 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 Authority has the power under Section 15.1 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 this power should not be unduly prescriptive. We recommend that this Section 15.1 be removed to mitigate against overly restrictive cross-border data transfer requirements that are likely to 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.

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 contract purposes, amongst others, which are also recognised under the Draft Bill as lawful grounds for processing personal data.

(ii) Specific drafting recommendations

In addition to the changes recommended to Section 15 of the Draft Bill in item 2.1(b) above which is also reflected below, we further recommend the following changes to Section 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 to which the data is being transferred offers personal data protection at least equivalent to the level of protection provided under this Act and that data so transferred shall be processed in accordance with this Act.

14.2 The requirements under sub-section (1) shall not apply where:

(a) the transfer is necessary for:

(i) the performance or conclusion of a contract, or implementation of pre-contractual measures;

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

(iii) important reasons of public interest;

(iv) 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 level of 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 requires the recipient to protect the personal data so transferred to a standard at least equivalent to level of 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 requires the recipient to protect the personal data so transferred to a standard at least equivalent to level of 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[1] recognized by the Authority which permits the transfer of Personal Data from Pakistan to the country in which the recipient is located.

2.3 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.

(i) Key issues and comments

The Draft Bill applies to all persons that process, have control over, or authorise the processing of personal data, where the data subject, data controller, or data processor are located in Pakistan. This is a departure from the July 2018 draft of the Bill which required data controllers and data processors established in Pakistan to fall within the scope of the Bill (territorial scope was limited to data controllers and data processors established in Pakistan). The present Draft Bill changes this position and expands its scope such that it is extra-territorial in nature.

This extraterritoriality is also wider than that under Article 3 of GDPR, which only applies to controllers or processors located outside of the EU where certain minimum thresholds are met (i.e. where the entity is actually offering goods or services to data subjects

[1] An example of international certification is the APEC Cross Border Privacy Rules System.

in the EU, or monitoring their behaviour). These thresholds do not exist in the Draft Bill and as long as the data subject is located in Pakistan, the Draft Bill would apply.

A clearly defined jurisdictional scope is important for both organisations and data subjects who seek to understand and manage their privacy obligations and rights. As currently drafted, the scope of the Draft Bill is such that it will apply to any data controller or data processor irrespective of location which processes the personal data of a single individual in Pakistan, and irrespective of the purpose of that processing (i.e. even if it is incidental). As it stands, the scope of application of the Draft Bill is impracticable and likely to cause jurisdictional conflicts.

As a result, the expanded scope 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 would clearly result in fewer benefits and choices to individuals in Pakistan and we therefore recommended that this extraterritorial scope in Section 3 be deleted.

Finally, we note that Section 3.3 of the Draft Bill contains a clarification on what types of persons are considered "established" in Pakistan for the purposes of "subsections (2) and (3)". We recommend clarifying that this should just refer to Sections 3.1 and 3.2 instead.

(ii) Specific drafting recommendations

Further to our comments and reasoning above, we suggest the following changes 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 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.*

2.4. The requirement to appoint a local representative should be removed and replaced with a narrower requirement that is based on a materiality threshold, similar to that under Article 27 GDPR and other International Benchmarks.

(i) Key issues and comments

The requirement in Section 3.2 for all data controllers and data processors not registered or established in Pakistan to have a local representative is possibly unnecessary and onerous. While the law can reasonably request a point of contact (or other mechanism to reach out) for the Authority and other agencies to inquire about privacy practices, Section 3 as currently written is overly prescriptive. It requires that the representative must be physically based in Pakistan. It is our opinion that such overly prescriptive requirements would unnecessarily burden businesses, and fail to meet MoITT's intended objective of ensuring that the Authority is able to reach the appropriate point of contact.

We recommend a materiality threshold for the appointment of a representative, similar to that under Article 27 of GDPR, where a representative is only required where the entity is offering goods or services to data subjects in that jurisdiction, or monitoring their behaviour. This approach would be more consistent with the position in the 2018 draft of the Bill where a representative was only required if equipment in Pakistan was used for processing personal data otherwise than for the purposes of transit. As currently drafted, this materiality threshold could also be achieved by narrowing the extraterritorial scope of the Draft Bill as recommended in item 2.3 above.

We also respectfully request greater clarity in the Draft Bill that the representative will not face personal liability for the acts or omissions of the relevant data controller or data processor. This lack of clarity may result in a significant barrier to entry for many global organisations, who arguably do not wish to place their employees and executives in such a high-risk position. We also suggest that the responsibilities of the representative be clearly defined either in the Draft Bill or regulations, so that organisations have greater guidance on who should be appointed to this role.

(ii) Specific drafting recommendations

In addition to the changes suggested under item 2.3 above which clarify the territorial scope and applicability of the Draft Bill, we further recommend the following changes to Section 3:

3. SCOPE AND APPLICABILITY *(…)*

3.2 A data controller or processor falling within clause (a) sub-section 1 ~~clause (a) of subsection (1) not registered/established in Pakistan~~ shall nominate for the purposes of this Act a representative ~~in Pakistan.~~, unless the processing undertaken by such data controller or processor is occasional, does not include, on a large scale, processing of sensitive personal data, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing.

~~*3.3 For the purposes of subsections (2) and (3), 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 The designation of a representative under sub-section (2) 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.

2.5. 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.

(i) Key issues and comments

Data protection officers, or "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 that the Authority 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.

(ii) Specific drafting recommendations

If MOITT's intention is to require the appointment of a DPO, we suggest that the 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.2 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.

2.6 The composition and responsibilities of the Authority should be further clarified and refined.

(i) Key issues and comments

Firstly, we recommend amending Section 32.4 of the Draft Bill to clarify the composition of the Authority. While the start of the Section mentions that the Authority will consist of seven members, the subsequent drafting in that section implies that possibly eleven members will be selected.

Secondly, we recommend deleting Section 34(2)(d) of the Draft Bill which grants the Authority the power to prescribe further regulations on "big / large data controllers / processors, along with other categories". It is unclear what definition will be applied to "big / large data controllers / processors" and what additional restrictions will be imposed on them, therefore generating significant uncertainty and costs around compliance obligations for businesses of all sizes. Best practices in data protection laws do not discriminate between data controllers or processors further to their size. Targeting large operators and imposing additional restrictions based on this criterion alone would be inconsistent with International Benchmarks and reduce legal certainty for organizations operating in Pakistan. In addition, such additional compliance

measures are unlikely to result in greater protection for data subjects, as many international players have in place longstanding global privacy programs which adhere to the hughes standards of privacy protections, often granting additional data protection rights and guarantees regardless of the location of the user.

Lastly, we understand that the MOITT intends to delete the Authority's power in Sections 34(2)(e) and (f) of the Draft Bill to implement a registration and licensing framework for both data controllers and data processors in Pakistan. We strongly agree with and commend the MOITT"s latest proposal to delete these powers from the Draft Bill. Implementing a registration and licensing framework would be out of step with most regional laws and International Benchmarks including GDPR, Singapore's PDPA, the OECD Privacy Guidelines and Australia's Privacy Act. This would be an unnecessary administrative burden for the local government, increase compliance cost for organisations (arising from the proposed registration fees and annual fees), and is unlikely to lead to meaningful increase in compliance by organisations or enhance individuals' privacy protections.

(ii) Specific drafting recommendations

In light of the comments and justification above, we recommend the following amendments to Sections 32 and 34 of the Draft Bill:

32. ESTABLISHMENT OF THE AUTHORITY

(...)

32.4 The Authority shall consist of ~~seven~~ nine members, ~~three~~ four of whom shall be an IT expert, a legal expert, a representative of civil society and a financial expert respectively, to be appointed by the Federal Government for a term of four years and who shall not be eligible for reappointment. The remaining five members shall be appointed as follows:

a) One ex-officio ~~M~~member shall be a representative of any one of the following:
- *i. Ministry of IT & Telecom*
- *ii. Ministry of Defence*
- *iii. Ministry of Interior*

b) One ~~regular~~ ~~M~~member (employee of the Authority) each from following sectors/areas:
- *i. Information and Communication Technology*
- *ii. Financial*
- *iii. Legal*
- *iv. Civil Society*

34. POWERS OF THE AUTHORITY

(...)

(2) In particular and without prejudice to the generality of the foregoing power, the Authority shall---

(...)

~~*d) Identify big / large data controllers / processors, alongwith other categories, and define special measures for compliance in accordance with the provisions of the Act.*~~

~~*e) Devise registration mechanism for Data Controllers and Data Processors.*~~

~~*f) Formulate a Licensing Framework for Data Controllers and Data Processors on Personal Data Protection in Pakistan.*~~

2.7 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.

(i) Key issues and comments

We support that MOITT has plans to remove "access control data" from the definition of "sensitive personal data" in Section 2(k) of the Draft Bill, which we agree with. Sensitive personal data is usually given a higher level of protection because its processing carries a higher risk to the privacy of individuals. 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 usernames and passwords that may not in many 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 same reason. Not all types of financial information are always higher risk to individual privacy and so a blanket inclusion of "financial information" would not be proportionate to the increased protection provided to 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.

We further recommend that the phrase "any other information for the purposes of this Act and the rules made thereunder" be deleted from the definition of "sensitive personal data". As mentioned above, clearly and precisely defining "sensitive personal data" is vital for certainty and compliance. It is crucial that all data controllers understand the scope of data that are subject to these additional requirements. A non-exhaustive definition of "sensitive personal data" in the Draft Bill creates uncertainty and makes it difficult for businesses to fully comply with the requirements. Furthermore, the inclusion of "any other information" renders void the intent of the Draft Bill to distinguish between personal data and other categories of data.

We understand that MOITT intends to amend the "and" at the end of Section 28.1(a) to "or" to make it clearer that the requirements of explicit consent in Section 28.1(a) and the other conditions in Section 28.1(b) are alternatives rather than cumulative requirements. We strongly support this change, which would bring the requirements for processing sensitive personal data more in line with International Benchmarks and best practice.

As currently drafted, the requirements of Section 28 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 28.1 are more specific than those in Section 5.2, we suggest that the words "Subject to" at the start of Section 28.1 be amended to read "Notwithstanding" to make it clearer that when processing sensitive personal data, only the requirements of Section 28 need to be complied with, and that the requirements under Section 5.2 only apply to the processing of non-sensitive personal data.

(ii) Specific drafting recommendations

In light of the above comments and in addition to the changes already proposed by MOITT on the latest industry call, we recommend the following amendments to Sections 2 and 28:

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 or religious beliefs~~, or any other information for the purposes of this Act and rules made thereunder~~.*

28. PROCESSING OF SENSITIVE PERSONAL DATA

28.1 ~~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—
(…)

2.8 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.

(i) Key issues and comments

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 Authority.

Prescriptive security standards may not reflect the state-of-the art regarding data security but are likely to increase compliance costs for organisations without resulting 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. Needless to say, data controllers and processors will carry the onus of and remain accountable for deciding on the appropriate security measures in the context of their processing activities. There is no "one-size-fits-all" solution, but data controllers and processors are well-positioned and equipped to make such decisions for their businesses.

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.

(ii) Specific drafting recommendations

Further to the suggestions and justifications above, we 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 reasonable 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~~.*
8.3~~4~~	*The data processor is independently liable to take steps to ensure compliance with security standards prescribed under sub-section (1).*

(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.

(i) Key issues and comments

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 for which it was collected for.

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, including for the establishment, exercise or defence of legal claims.

To accommodate the above, inspiration can be taken from Singapore's PDPA, which permits organisations to retain personal data where it is necessary for any legal or business purposes.

(ii) Specific drafting recommendations

In light of the comments and issues raised 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, and the situations in Section 24 where personal data may be disclosed for other purposes should be clarified.

(i) Key issues and comments

There is a general prohibition in Section 12.1 on personal data being transferred to "any unauthorised person or system". 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 consider that such confusion may not have been intended as this section appears to have been accidentally retained from the December 2018 draft of the Bill. We therefore recommend that Section 12.1 be deleted in its entirety.

(ii) Specific drafting recommendations

Further to the comments above, we suggest that the following changes be made to Section 12 of the Draft Bill:

12 ~~TRANSFER OF PERSONAL DATA~~ NOT USED

~~12.1 Personal data shall not be transferred to any unauthorized person or system.~~

(...)

2.9 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, and the timeline for complying with an exercise of the right in Section 27 should have more flexibility.

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

(i) Key issues and comments

There is no clarity as to what "unwarranted" and "substantial damage or distress" entails, which is likely to result in excessive and unfounded 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 substantial range of data protection rights consistent with best practices. In particular, the rights to correct and erase personal data, as well as the right to withdraw consent to processing operations, are sufficiently framed to ensure a high and additional level of user control over their data in line with accepted International Benchmarks.

(ii) Specific drafting recommendations

25 ~~***RIGHT TO PREVENT PROCESSING LIKELY TO CAUSE DAMAGE OR DISTRESS***~~ ***NOT USED***

~~*25.1 Subject to subsection (2), a data subject may, at any time by notice in writing to a data controller, referred to as the "data subject notice", require the data controller at the end of such period as is reasonable in the circumstances, to —*~~

~~*a) cease the processing of or processing for a specified purpose or in a specified manner; or*~~
~~*b) not begin the processing of or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject if, based on reasons to be stated by him —*~~
~~*i. the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or a relevant person; and*~~
~~*ii the damage or distress is or would be unwarranted.*~~

~~*25.2 Subsection (1) shall not apply where —*~~
~~*a) the data subject has given his consent;*~~
~~*b) the processing of personal data is necessary —*~~
~~*i. for the performance of a contract to which the data subject is a party;*~~
~~*ii. for the taking of steps at the request of the data subject with a view to entering a contract;*~~

~~iii. for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by contract; or~~

~~iv. in order to protect the vital interests of the data subject; or~~

~~c) in such other cases as may be prescribed by the Federal Government upon recommendations of the Authority through publication in the Official Gazette.~~

~~25.3 The data controller shall, within twenty-one days from the date of receipt of the data subject notice under subsection (1), give the data subject a written notice –~~

~~a) stating that he has complied or intends to comply with the data subject notice; or~~

~~b) stating his reasons for regarding the data subject notice as unjustified, or to any extent unjustified, and the extent, if any, to which he has complied or intends to comply with it.~~

~~25.4 Where the data subject is dissatisfied with the failure of the data controller to comply with the data subject notice, whether in whole or in part, under subsection (3) (b), the data subject may submit a complaint to the Authority to require the data controller to comply with the data subject notice.~~

~~25.5 Where the Authority is satisfied that the complaint of the data subject under subsection (4) is justified or justified to any extent, the Authority may require the data controller to take such steps for complying with the data subject notice.~~

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

(i) Key issues and comments

The intent of the provision is unclear. We respectfully request greater clarity on the motivations for including "right of foreign data subjects", since the scope of application of the new law does not differentiate between national and foreign data subjects and should be limited to the activities of controllers and processors established in Pakistan as discussed in item 2.3.

As currently drafted, Section 26 creates uncertainty in respect of the obligations that data controllers in Pakistan would have to comply with. This raises additional concerns about the extraterritoriality of the Draft Bill. If the legislator were to overlook the recommendations proposed under item 2.3 on limiting the territorial application of the law, there would be a risk that Section 26 could be construed so as to impose obligations globally on any controller or processor subject to the Draft Bill. We reiterate our concern with this approach, which is likely to give rise to multiple jurisdictional conflicts and is not interoperable with foreign data protection laws to which many companies are equally subject.

(ii) Specific drafting recommendations

26 ~~RIGHTS OF FOREIGN DATA SUBJECTS~~ NOT USED

~~*Foreign data subject shall have all his rights, if any provided under the laws of the country or territory where the foreign data has been collected or data subject resides in so far as consistent with this Act..*~~

(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.

(i) Key issues and comments

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 much shorter than those found in international Benchmarks and would pose a significant, if not insurmountable, administrative burden for businesses, in particular small enterprises. We encourage the legislator to rethink the introduction of prescriptive timelines and consider whether it is sufficient, in line with best practices, to introduce an obligation to respond to a request for erasure "as soon as reasonably possible" or "promptly". The latter approach recognises that 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.

(ii) Specific drafting recommendations

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:
(…)
Note: In the GDPR, "Undue delay" is considered to be about a month with ability to extend for up to 2 months.

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

(i) Key issues and comments

While we note that several criminal fines and sanctions have been removed since the 2018 draft of the Bill, criminal liability for any breach of the processing and disclosure requirements is still imposed in Section 41 of the Draft Bill (as well as in Sections 23 and 44), while the quantum of fines has been substantially increased in Sections 23, 41, 42, 43 and 44 as well.

Section 44 of the Draft Bill further 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 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 also recommend an alignment with the GDPR, which focuses on liability of controllers and processors for damages caused by non-compliance.

(ii) Specific drafting recommendations

In light of the above comments and justifications, we propose the following changes to Sections 23, 41 and 44 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~~.

(...)

41 UNLAWFUL PROCESSING OF PERSONAL DATA

41.1 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.

41.2 ~~*In case the offence committed under sub-section (1) relates to sensitive data the offender*~~ *Anyone who processes or causes 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.*

(…)

44 CORPORATE LIABILITY

44.1 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.*~~

3. CONCLUSION AND NEXT STEPS

We appreciate the opportunity to contribute to the future of data protection in Pakistan. The summary above is not an exhaustive list of our concerns and recommendations in respect of the Draft Bill. There are other aspects of the Draft Bill that require further consideration in order to find the right balance between the rights of data subjects, and broader social, economic and innovation-related objectives.

While we reiterate our support for Pakistan's efforts to introduce personal data protection legislation, we respectfully encourage MOITT to engage in further dialogue with industry to consider the broader issues and implications, before the Draft Bill is finalised.

We would welcome an opportunity to contribute further to these discussions and the wider development of the Draft Bill, including to join any applicable industry working groups and to engage in further dialogue with MOITT.

We look forward to hearing from you as to any opportunities we may have to contribute further in this respect.

***** END OF SUBMISSION *****