12 June 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

Dear Minister Syed Amin Ul Haque,

On behalf of the Asia Internet Coalition (**"we, us, AIC"**) and its members, we would like to express our sincere thanks to the Ministry of Information Technology and Telecommunication (**"MoITT"**) for giving us the opportunity to provide our feedback on the Public Consultation on Pakistan's Data Protection Bill 2020 (the "**Draft Bill**"). As an introduction, the AIC is an industry association that promotes the understanding and resolution of internet policy issues in the Asia Pacific region. Our members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media). We have worked closely with the governments around the region 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 wish to share that the AIC has been actively engaging with the Government of Pakistan on key policies such as the Citizens' Protection Rules, Pakistan Electronic Media Regulatory Authority Regulation on Web TV and Over the Top TV as well as Pakistan's Digital Taxation Framework, to which we have submitted recommendations and best practices, ensuring that the industry voice is reflected in the regulatory approach.

Now is an opportune time for Pakistan to develop a framework for personal data protection. As technological advancements continue to evolve and become more sophisticated, so do the threats. This rings particularly true given the current COVID-19 pandemic, due to which a great deal of our lives has been moved online. Therefore, it is now more critical than ever to protect individual data, particularly when economies and companies are transitioning rapidly into the digital space.

That being said, we are concerned that certain aspects of the Draft Bill – particularly those relating to data localization – will adversely impact Pakistan's digital ambitions. As outlined in comments below, the data localization requirements in the Draft Bill will undermine privacy and data security and stifle innovation and growth in technology and internet-dependent industries. As such, please find appended to this letter along with detailed comments and recommendations, which we would like to respectfully request the Ministry of Information Technology & Telecommunication to consider in preparing the Data Protection Bill. We have

highlighted the most critical issues corresponding to the sections, followed by other issues and accompanying recommendations. Critical issues include:

1. Sections 14 and 15: Data Localization and Cross-Border Data Flows
2. Section 3: Extra-territorial scope
3. Section 3: Data Protection Officer (DPO) and local representative requirements
4. Section 34: Overbroad Powers for the Data Protection Authority
5. Section 2: Definition of "Sensitive Personal Data"
6. Section 7, 8, 9, 12, 24, 28: Conditions for processing personal data (Chapter II) and sensitive personal data (Chapter IV)
7. Section 8: Security Requirements
8. Sections 16, 20, 25, 26, 27: Rights of Data Subjects
9. Sections 23, 41, 44: Criminal penalties and fines

Should you have any questions or need further clarification, please do not hesitate to contact me directly or our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or +65 8739 1490. Furthermore, we would also be happy to offer our inputs and insights on industry best practices, directly through meetings and discussions and help shape the dialogue for the advancement of the digital economy goals of Pakistan.

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)

Detailed Comments and Inputs Pakistan Personal Data Protection Bill

A. INTRODUCTION

The protection of personal data is an important component of any privacy framework and we appreciate the opportunity to provide feedback on the Draft Bill. We appreciate the efforts of MoITT to work towards implementing a holistic framework for the protection of personal data since the initial release of the draft legislation in 2018.

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. Employing data protection to enable a dynamic digital economy which protects consumers and facilitates Pakistani enterprises;
2. The promotion of data-driven innovation; and
3. Ensuring 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 its current form, the **Draft Bill** falls short of these goals, and may adversely impact Pakistan's digital ambitions and make it difficult for foreign companies to operate and offer services seamlessly to Pakistani businesses and users.

B. COMMENTS AND RECOMMENDATIONS ON KEY SECTIONS

B.1. Critical Issues

1. Sections 14 and 15: Data Localization and Cross-Border Data Flows

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, secured by appropriate technologies. It is well-recognised that data flows are a significant contributor to the success of modern globalised economies.

Despite this, the Draft Bill includes two sweeping data localization provisions. Section 14.1 requires that "*Critical Personal Data*," a category of data which, problematically, is not defined, must be processed and stored solely within the borders of Pakistan. Additionally, PDPA 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. Section 15.2 requires PDPA to introduce a data localization framework to force companies to store copies of personal data in Pakistan, even where that data may otherwise be transferred out of the country.

These requirements will undermine privacy and data security, stifle innovation and growth in technology and internet-dependent industries, and will not address challenges Pakistan law enforcement faces in obtaining digital evidence for criminal investigations. We recommend that the requirements for data localization and the concept of "critical personal data" be removed from the Draft bill.

a. Forced data localization undermines business

Forced data localization harms businesses from every sector and stifles trade. Most businesses today, including traditional sectors such as agriculture and manufacturing, rely on data to manage global operations, and data flows contribute significantly to economic growth and digital trade. In fact, a McKinsey report states that global data flows contributes $2.8 trillion to annual trade, and contributes a larger share of the increase in global GDP compared to the global trade in physical goods. The inability to move data freely across geographies creates a major impediment to efficiency, productivity, and costs. A report by the European Centre for International Political Economy (ECIPE), for example, found that data localization would reduce GDP by 0.8% in Brazil, 1.1% in China, Korea, and the EU, 0.8% in India, 0.7% in Indonesia, and 1.7% in Vietnam.

Competing on the global stage means companies need cutting edge tools, reliable infrastructure that can scale globally, and access to a diverse customer base. Forced data localization laws artificially limit the ability of companies, especially small and medium enterprises, to access the best available tools, support employees, customers, and users in multiple regions around the world, thereby limiting growth opportunities.

This is especially important in the context of Pakistan, whose IT sector presents a bright spot in the economy. According to the Pakistan Software Houses Association for IT and ITeS (P@SHA), the IT sector of Pakistan is the second largest exporter of the country with more than 24% growth over the last eight months, more than any other sector of the country. P@SHA also estimates that Pakistan produces 23,000+ IT graduates every year, who are employed by over 7,000 IT companies. And according to a report by Invest2Innovate and the World Bank Group, Pakistan's startup ecosystem has been growing quickly and now features over 1000+ startups, 24 incubators and accelerators and 80 co-working spaces.

The data localization provisions contemplated in the draft bill would make it difficult for these start-ups to provide services and expand in global markets. For example, they would make it difficult for Pakistani companies to gain access to innovative technologies like data analytics, artificial intelligence and machine learning tools, etc. that depend on data flows. They may also lose access to cost-efficient cloud services in the global market.

Cross-border data flows will be a critical enabler for Pakistan's economic recovery post COVID-19. Companies of all sizes and sectors have relied on digital services and

remote working tools to continue running their business during the crisis, and will continue to use these services going forward. Cloud-driven services provide companies with the flexibility and reasonable cost structure to scale up or down according to their business needs. Many digital services are run on global and regional networks and it is therefore important for Pakistan to put in place a progressive data governance framework that allows for cross border data flows as much as possible. Pakistani businesses, especially SMEs that rely on internet-enabled trade, will be the key beneficiaries of enabling policies that promote cross-border data flows.

b. Forced data localization will undermine Pakistan's trade goals

Recognising the central role cross-border data flows play in enabling global digital trade and e-commerce, recent global and regional digital trade agreements (CPTPP, USMC Agreement, etc.) have prohibitions against data localization. Pakistan's trade partners in the Asia Pacific region, including Japan, Australia, and Singapore, have already taken on binding commitments to allow for cross-border data flows to boost their digital economies. Therefore, the Draft Bill should be amended keeping in mind the development of Pakistan's digital trade strategy, the need to maintain economic competitiveness and to create an enabling environment for Pakistani digital exporters to access foreign markets.

c. Forced data localization undermines privacy and security

Strict restrictions on the cross-border processing and/or storage of data are not the best way to protect people's privacy. The US Federal Trade Commission and the European Commission have publicly warned against data localization 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.

It is evident that requiring data to be exclusively stored in one location may actually put users' privacy and security at greater risk. 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. Given the nature of distributed networks, a company that complies with local or regional (e.g., EU) laws will do so regardless of the location where its data is stored. Distributed networks prove critical to increasing resilience and enabling back-up service in the event of a network failure. In some cases, an outage could impact enough of the local infrastructure that any data that was exclusively stored locally could be destroyed or made inaccessible.

Since data localization imposes significant data storage costs for companies of all sizes, such companies will be less likely to invest in state-of-the-art network protection tools. This is because compliance with data localization 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 centralization of

data storage, leave people's data more vulnerable to unauthorized access, exfiltration, and exploitation by malicious actors such as criminal hackers and foreign spies.

Where no data localization 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 decentralize where sensitive or personal data are stored to ensure it is harder for malicious actors to find and access. Increasingly, we see many companies, large and small, rely on cloud storage solutions for their data management because it allows an affordable and scalable way to deploy the latest technology and tools across the network to make it secure. This is not possible with data localization.

In addition, financial institutions and other firms rely on cross-border data flows to conduct cutting edge compliance and security protocols, including pattern analysis to detect fraud. This has led the U.S. Department of Treasury to state that forced data localization may "increase cybersecurity and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information." Similarly, a report by the GSMA's Mobile Money programme found that "The implementation of data localisation requirements can have unintended consequences leading to reduced data security, increased money laundering / terrorist financing risks and even the closure of services."

d. Forced data localization does not facilitate law enforcement access

Regardless of the location where data is stored, U.S. companies are subject to U.S. law, which places strict limits on their ability to disclose data, subject to certain exceptions. As the U.S. Department of Justice has concluded, "data location is often not a good basis upon which to ground requests to produce electronic data." Pakistan should consider diplomatic channels, such as signing an Mutual Legal Assistance Treaty (MLAT) or acceding to the Budapest Convention, which would help them obtain data through the appropriate channels.

In addition, Pakistan should consider the development of a single point of contact for government-to-government requests, ensuring that requesting agencies are familiar with the standards of US law and have reviewed requests to ensure they meet US standards. Finally, it should be noted that many US companies have processes for responding to and granting emergency disclosure requests, and that many such requests from Pakistan have been granted.

e. The bill should facilitate cross-border data flow *while* protecting privacy.

The Draft Bill must facilitate cross-border data flows, while protecting individuals. We strongly recommend that the requirements for data localization be removed from the Draft Bill. 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.

To ensure accountability, we recommend MoITT consider, and explicitly recognize in the Draft Bill as permitted cross-border transfer mechanisms, proven approaches

such as 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 CBPR"),.

The bill should also set out minimum protections (e.g. Singapore PDPC's guidance) which should be in the scope of every contract governing overseas data transfer. Alternatively, MoITT can consider publishing one or more sets of approved standard contractual clauses which can be used by companies 'off the shelf', as the European Commission has done. 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.

1.1. Critical personal data

The Draft Bill allows the Government to notify certain categories of personal data as "critical personal data" (CPD). According to Section 14.1, CPD must be processed *only* in Pakistan. **At present the Draft Bill lacks clarity in the scope of CPD in the following respects:**

1) it does not provide any definition of CPD;
2) it does not specify any parameters or criteria for classification of CPD; and
3) the government can notify categories of CPD, without consulting either the future Draft Bill, or industry, who will be significantly impacted.

We recommend that the concept of "Critical Personal Data" be removed from section 2(o) and the rest of the Draft Bill. The separate concept of "Critical Personal Data" does not align 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. Section 14.2 grants the federal government an overbroad ability to designate certain categories of personal data based on vague and undefined "grounds of necessity or strategic interests of the State."

The definitional ambiguity could result in sweeping exclusions from cross-border data transfers and huge 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", is also extremely burdensome, if not wholly impossible to comply with.

The intended purpose of the PDP Bill is to provide a framework of rights and interests of data subjects in order to better protect their privacy and personal data. 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).

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 drafting be clarified as to which subsection this was intended to refer to, as it currently refers to itself.

2. Section 3: Extra-Territorial Scope

Section 3 of the Draft Bill states that the Act would apply to any person who "Processes, has control over or authorises processing of any personal data if the data subject, controller or processor (local or foreign) is located in Pakistan."

This is a departure from the July 2018 draft Bill, which required data controllers and data processors established in Pakistan to fall within the scope of the Draft Bill. The present Draft Bill changes this position and expands its scope such that it is extra-territorial in nature. 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 minimum thresholds are met (i.e. where the entity is actually targeting the sale of goods or services to data subjects 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.

Extra-territorial application as contemplated in Section 3 unnecessarily hampers the growth of new businesses and creates conflicts of law between jurisdictions. In particular, small businesses shouldn't have to worry about running afoul of foreign regulators merely because a few people from another country navigate to their website or use their service. This is unnecessarily burdensome and poses barriers for small businesses to engage in cross-border digital trade.

Data protection law should adhere to established principles of territoriality, regulating businesses to the extent they are actively doing business within the jurisdiction. 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 – that processes the personal data of a single individual in Pakistan. This presents a severe operational burden, as it is difficult, if not impossible in many cases, for companies to geo-locate their customers. This provision would also appear to run counter to established principles of data minimization, to the extent that it would require companies to determine where their customers are physically located at any given moment. The expanded scope of extra-territoriality could 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. We therefore strongly recommended that this extraterritorial scope in Section 3 be deleted or considered in alignment with the provision under GDPR (including the clarifications in Recital 23 and Article 3 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.

Instead, the law should allow for interoperability consistent with global norms. This will make it less onerous to operate businesses regionally or globally, and will demonstrate a modern approach to governing data protection. Trade agreements increasingly focus on addressing regulatory fragmentation by encouraging adherence to or alignment with regional data protection standards, while preventing restrictions on cross-border data flows. The USMC Agreement, for instance, references the APEC CBPR. By focusing on interoperability rather than extra-territorial reach, governments can reduce barriers to cross-border digital trade and ensure that small businesses have the opportunity to participate in the global digital marketplace.

3. Section 3: Data Protection Officer (DPO) and local representative requirements

Data protection officers, or "DPOs", play an important role in ensuring an organization complies with privacy laws and facilitating the exercise of data subject rights. Section 3 requires foreign data controllers and processors who are "not registered/established in Pakistan" to appoint a representative in Pakistan. While the law can reasonably request a point of contact (or other mechanism to reach out) for the Personal Data Protection Authority and other agencies to ask questions about privacy practices, Section 3 as currently written is unnecessary and onerous. It requires that the representative must be physically based in Pakistan. Such overly prescriptive requirements would unnecessarily burden businesses, and will not meet MoITT's intended objective of ensuring that PDPA is able to reach the appropriate point of contact.

Internationally, best practice in this area provides for flexibility in allowing organizations to choose who acts as the DPO. This enables organizations to appoint an individual or group of individuals who will act as the DPO in a way that best reflects the organization's structures and processes. For example, smaller organizations may only wish to appoint one individual as its DPO due to the size and scale of the business. Multinational organizations, however, may wish to appoint a centralized team as its DPO oversees privacy across multiple markets due to the scale of the organization and their processing of personal data. This team can still respond to reasonable requests as per applicable legislation in a timely manner, without having a local representative physically located in each jurisdiction.

As currently drafted, the requirement to appoint a DPO in Pakistan is overly onerous. One of the criteria for types of persons considered "established" in Pakistan creates a legal fiction for 'establishment in Pakistan' on the basis of extremely broad and undefined terms such as '*carries on any activity*' and *'regular practice*'. To ensure clarity around legal terminology related to establishment, we would recommend that Section 3.3(d) be deleted. We further recommend a materiality threshold for the appointment of a local representative, similar to that under Article 27 of GDPR, where a local representative is only required where the entity is offering goods or services to data subjects in the EU, or monitoring their behaviour. This approach would be more consistent with the position in the 2018 draft of the Bill where a local 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 above. Finally, we also note that Section 3.3 of the Draft Bill contains a clarification on what types of persons are considered "*established*" in Pakistan. This currently refers to "subsections (2) and (3)", which appears to be a drafting error. We recommend clarifying that this should just refer to Section 3.2 instead.

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 as this would be a significant barrier to entry for many global organisations that do not wish to place their employees and executives in such a high-risk position. We also suggest that the roles and the scope of responsibilities of the representative be clearly defined either in the Draft Bill or in subsidiary legislation, so that organizations have greater guidance on who should be appointed to this role.

4. Establishment of PDPA and Powers for the Data Protection Authority

4.1. Section 32: Establishment of PDPA

We note that while previous drafts of the Draft Bill contemplated the establishment of a Commission, this latest draft proposes the establishment of a statutory authority referred to as the Personal Data Protection Authority ("PDPA") of Pakistan. We urge that the composition and responsibilities of PDPA should be further clarified and refined. Firstly, we recommend amending Section 32.4 of the Draft Bill to clarify the composition of PDPA. While the start of the Section mentions that PDPA will consist of seven members, the subsequent drafting in that section implies that ten members will be selected.

It is prudent for the Draft Bill to create some form of enforcement agency, authority, or commission specifically tasked with developing subject-matter expertise on data protection. However, we notice that previous versions of the Draft Bill included the following clauses regarding the composition of the Authority/Commission, which have been removed from the latest version:

a) One Commissioner shall be a person who has been or is qualified to be a judge of High Court;
b) One Commissioner shall be a person having [a] master degree in computer sciences or telecommunications and fifteen years of experience in the field of information technology, telecommunications or computer sciences.

We would recommend that these clauses be re-included in the Draft Bill, so as to ensure appropriate technical expertise and oversight.

The Federal Government has been given the power to appoint all the members of PDPA. This could allow the Government to influence the composition of PDPA and exercise control over its decision making, compromising the independence of PDPA. In order to avoid this and ensure transparency, the manner of selection of members should be clearly prescribed and/or a selection committee must be appointed.

Moreover, Section 32.8 should be amended to ensure that the Federal Government is not permitted to vary the salary and other terms of service of the members of PDPA.

4.2. Section 34: Overbroad Powers for the Data Protection Authority

The powers granted to the PDPA in Section 34 are overly broad and insufficiently defined. Of particular note are:

- Subsection 34(2)(d), which requires the PDPA to "identify big / large data controllers / processors, along with other categories, and define special measures for compliance in accordance with the provisions of the Act." No indication is provided as to what these special measures might entail, how the threshold for "big/large" would be defined, nor the reason why such requirements would be necessary. International best practice is to differentiate legal requirements based on the data being collected, rather than the company collecting the data. As such, we recommend that this subsection be removed.

- Subsections 34(2)(e)-(f), which requires the PDPA to devise frameworks for registration and licensing of Data Controllers and Data Processors. Similarly, no details are provided regarding the purpose of these requirements, nor what the registration and licensing frameworks would entail. We recommend that PDPA'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 be deleted. 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 government, increase compliance cost for organisations (arising from the proposed registration fees and annual fees), and may not lead to meaningful increase in compliance by organisations or enhance individuals' privacy protections.

Vague provisions such as those found in subsection 34(2) that hint at undefined "special measures" and registration/licensing frameworks risk creating uncertainty and apprehension about the ease of doing business in Pakistan, thereby stifling foreign trade and investment. What's more, such provisions have no clear connection to the goal of ensuring that user data is protected. If the goal behind such provisions is to enable the PDPA to conduct enforcement actions and issue penalties and other remedies, such measures can be taken without imposing registration and licensing frameworks. GDPR, for example, does not impose such requirements on data controllers and processors.

5. Section 2: Definition of "Sensitive Personal Data"

To improve clarity and reduce uncertainty for businesses, we 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". Clearly and precisely defining "sensitive personal data" is important given the additional requirements imposed on the processing of such data. 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.

Moreover, the inclusion of access control data and financial information in the list of sensitive personal data is out of line with global practices as these categories of data are typically not accorded a special care category status, such as sensitive personal data, under global data protection regimes. Further, requiring explicit consent and additional conditions to process “access control data” and “financial information” is impractical operationally, has adverse implications on the ease of doing business, and is out of line with international norms. This requirement inhibits many ordinary uses of such data – such as instances where its processing would clearly benefit the data subject, instances where the privacy risks are limited, the data subject could reasonably expect the processing, consent cannot be obtained and data subjects would unlikely object to the processing (e.g., authenticating users of a service or processing previously agreed recurring payments). A requirement for explicit consent for such processing could also lead to consent fatigue, a well-recognized phenomenon which notes that data subjects feel harassed by constant notices seeking consent, and are therefore likely to reduce the use and adoption of digital services. This would have a cascading impact on existing business models in marketing, consulting, fintech, all manner of services provided online and on the adoption of new technologies such as AI. This would ultimately impede innovation and economic development in Pakistan, as these industries will likely migrate to countries with favourable transactional regimes that also provide for personal data protection. We, therefore, recommend that “access control data” and “financial information” be excluded from the SPD category.

6. Section 7, 8, 9, 12, 24, 28: Conditions for processing personal data (Chapter II) and sensitive personal data (Chapter IV)

6.1. Processing of Personal Data

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 PDPA.

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.

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.

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

The Draft Bill should also provide exceptions to this requirement where it is not technically feasible to comply, or where deletion/destruction would prevent organisations from performing a contract or providing a service requested by a user, if the data is retained for disaster recovery or legal/compliance 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.

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.

We also recommend further clarity in relation to the circumstances in Section 24(c) and (d) of the Draft Bill which permit disclosure of personal data for other purposes based on the "reasonable belief" of the data controller. We suggest that additional detail on what constitutes a "reasonable belief" could be provided for in subsidiary regulations and guidance.

6.2. Processing of Sensitive Personal Data

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.

Section 28 of the Draft Bill lists down the conditions for processing of sensitive personal data on the explicit consent of the data subject in addition to one of nine other enumerated requirements. As drafted, this Section is also subject to Section 5 (2), which provides for a number of legal bases for the processing of personal data.

In the first instance, this reference to Section 5 creates significant confusion and uncertainty regarding under which basis data controllers may process categories of personal data. We recommend that this reference to Section 5 be deleted from Section 28.

Furthermore, the requirement on data controllers to obtain both explicit consent and to meet one of the nine listed requirements in order to process sensitive personal data will have the net effect of prohibiting the processing of a vast percentage of personal data. This will severely inhibit the ability for businesses to provide services to Pakistani users, to innovate and to grow as part of the modern developing digital economy in Pakistan. This will be particularly acute for indigenous enterprises. The onerous requirements in Section 28 are also completely out of alignment with any other international benchmarks regarding the processing of sensitive personal data (e.g. Article 9 GDPR). The effect of this will be to prevent businesses from processing such data even if a user consents but none of the other listed requirements are met. To align with best practice and to address these significant issues, we recommend that Section 28 be amended to require explicit consent be made as one of the parameters for processing SPD, as opposed to making it a mandatory condition along with expanding the grounds for processing of sensitive personal data by borrowing certain grounds from Article 9 of GDPR.

7. Section 8: Security Requirements

Section 8 of the Draft Bill imposes an obligation on data processors to implement security safeguards. This is at odds with the role of a data processor, which is to process personal data based on the instructions of, and on behalf of a data controller.

Data processors do not have control over the data or visibility over the nature, scope and purpose of processing of such data, and are unable to ascertain the likelihood of harm. Data processors are therefore not in a position to make meaningful or independent decisions about the collection, usage, processing or disclosure of personal data - rather their scope is limited to only implementing the decisions of the data controller. Therefore, the responsibility for determining and implementing security safeguards should be vested solely with the data controller and should not be extended to data processors. We, therefore, recommend that the references to data processors should be removed from Section 8.3 and 8.4.

Further, we recommend deleting the requirement in Section 8.1 of the Draft Bill to comply with specific security standards which will be prescribed by the Authority on the basis that 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, and based on best industry practice. The requirements 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 in itself would be sufficient and is reflective of International Benchmarks.

8. Sections 16, 20, 25, 26, 27: Rights of Data Subjects

We support giving individuals the ability to access, correct, delete and download personal information about them. Individuals should have access to personal information they have provided to an organization, and where practical, have that information corrected, deleted, and made available for export in a machine-readable format. This not only empowers individuals, but it also keeps the market innovative, competitive, and open to new entrants.

However, we recommend that the law include flexible balancing mechanisms or exceptions to enable businesses to consider access, correct, deletion requests against legitimate business purposes for retaining data. Specifically, we would recommend that Section 20.1(c) and 27.2 be amended to include sufficient safeguards (such as technical infeasibility and disproportionate effort) for data controllers that act on a data subject's request.

We also recommend the deletion of the following sections:

- Sections 16.4 and 19.2: The intent behind these subsections is unclear. We are not aware of any situation whereby a data controller would "control the processing of

the personal data in such a way as to prohibit the data controller who holds the personal data from complying with the data access request." As such, we recommend deletion of this clause unless it can be clarified.

- Section 20.5: The first data controller may not be in a position to identify "another data controller that is in a better position to respond to the data correction request." Thus, there shouldn't be an obligation on the first data controller to route the request to any other data controller. It would be more effective if the data subject were responsible for transferring this data instead and the privacy concerns would be sufficiently addressed by the ability to download the data.

- Sections 25 (right to cease processing due to unwarranted and substantial damage or distress)**:** 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.

- Section 26 (right for foreign data subjects provided)**:** The intent of the provision is unclear and we respectfully request greater clarity on the motivations for including this. Furthermore, 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.

Further, there should be more flexibility 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 organizations prioritize 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.

9. Sections 23, 41, 44: Criminal penalties and fines

While we note that several criminal fines and sanctions have been removed since the 2018 draft of the Draft 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 23 imposes potential criminal liability on data controllers for any processing of data after withdrawal of consent by a data subject, apart from a fine up to 5 million Rupees. Such criminal penalties run contrary to established international standards under data protection regimes. Criminal liability presents disproportionately harsh consequences considering the nature of contravention, and could disincentivize companies from investing further in a market or naming representatives that hold decision-making power.

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 organizations 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 organizations as it incentivizes 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.

B.2. Additional Issues and Accompanying Recommendations

1. Section 1: Transition Period

The Draft Bill currently provides for a period of between 1 to 2 years for the enforcement of its provisions. Given that the Draft Bill establishes a comprehensive data protection framework for the first time in Pakistan, organizations – including

small and medium businesses and start-ups will have to re-architect their technical systems and processes in order to comply with the Draft Bill's provisions. Doing so under a timeline that is unclearly worded is likely to pose a challenge for organizations. Notably, global frameworks such as the GDPR provided a 24-month window to entities for compliance. Therefore, we recommend that Section 1.3 of the Draft Bill be amended to provide for a clear transition period of a minimum of 24 months beginning from the date that the relevant rules are issued (but not from the date of when the Act is promulgated) to enable entities to comply with provisions.

2. **Section 13: Personal Data Breach Notification**

The Draft Bill places the primary duty of notifying the Data Protection Authority regarding data breaches, on the data controller. However, it also states that Data Processors would also be subject to these obligations if they "become aware" of a personal data breach. The provision has overlooked the fact that data processors only process data on behalf of data controllers, with whom they typically engage through a contractual relationship. The processor may therefore not have the necessary control over the data or be able to furnish details regarding the nature of the breach sought by the reporting mechanism proposed.

Additionally, mandating both the controller and the processor to report breaches could result in erroneous or conflicting reporting of a breach, and create confusion on the nature of the breach. In order to streamline this process, we recommend that section 13.5 be amended to mandate data processors to report personal data breach only to the data controller upon becoming aware of a breach. The ultimate and sole responsibility of notifying this to PDPA or affected data subjects must lie with the data controller.

We recommend that the term "data breach" is defined, and guidance provided on the kinds of breaches likely to result in "a risk to the rights and freedoms of a data subject" in order to provide clarity for organisations assessing whether an incident is notifiable or not.

3. **Section 22: Notification of refusal to comply with data correction request**

Section 22.2 is a matter of concern. It is unclear what steps and in what manner a data controller has to "make a note" to indicate that the personal data is disputed by the data subject, nor how the data controller should determine whether the personal data is an "expression of opinion." We would respectfully request removal of this provision. If at all retained, it would be helpful to have clarity on how data controllers should retain or store the note and for how long, so that we can provide feedback as needed.

4. **Section 30: Exemptions**

The wording of Section 30.2 is ambiguous and seems to indicate that the exemptions do not apply to Sensitive Personal Data and Critical Personal Data. We recommend

replacing the phrase "Subject to section [28] and critical personal data, personal data" with "The following personal data is exempt from requirements of Sections 5, 6 and 7 of the Act."

5. **Section 38: Powers of the Federal Government to issue Policy Directives**

PDPA should be permitted to function autonomously and independently, except in very specific and exceptional circumstances. The obligation of PDPA to comply with all the directions of the Federal Government on questions of policy is a very broad power given to the Federal Government and may result in PDPA being subject to the whims of the Federal Government from time to time.

This power should be balanced by the responsibility of the state to conduct extensive public stakeholder consultations before the notification of such directives as described in section 38.1. Carrying out a consultation process will ensure that the Federal Government takes into consideration the comments of various stakeholders before notifying the rules, thereby allowing them to formulate subordinate legislation which is practical and in consonance with the prevalent global practices.

Moreover, if PDPA decides to adopt the directives issued by the Federal Government, they should be adopted in a timely manner (e.g. within six months of issuance of the directives) taking into account the impact of the implementation of such directives on businesses.

6. **Sections 45 and 46: Complaints and Appeals**

Section 45.1 empowers "any individual or relevant person" to file a complaint regarding violations of data subjects' rights or breach of data controllers'/ processors' obligations under the Act. This may lead to a large number of possibly overlapping complaints, creating operational issues for data controllers and the PDPA alike, as well as a high level of uncertainty. As such, we suggest that the term "any individual or relevant person" should be replaced with "any aggrieved person."

We also recommend that Section 46 be amended to indicate that decisions of the PDPA may only be appealed by a party aggrieved within a specified timeframe after the decision (e.g., within 30 days from receipt of a certified copy of the order).

CONCLUSION

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.