U.S. CHAMBER OF COMMERCE

U. S.-PAKISTAN BUSINESS COUNCIL

September 16, 2021

The U.S. Chamber of Commerce and the U.S.-Pakistan Business Council (USPBC) appreciate the opportunity to provide further comments on the Draft Pakistan Personal Data Protection Bill 2021.

This builds on our previous comments submitted to Federal Minister for Information Technology and Telecommunication (MoITT) Dr. Khalid Maqbool Siddiqui in October 2019 and to Minister of Information Technology and Telecommunication Syed Amin Ul Haque and Adviser to the Prime Minister of Pakistan on Commerce and Investment Razak Dawood in October 2020. We also provided comments to MoITT officials in April 2021 following the USPBC virtual discussion with Member IT and Member Legal earlier that month. We appreciate the efforts made by the Government of Pakistan to take some of our previous recommendations into consideration.

The Chamber and USPBC share Pakistan's goal of enhancing international commerce, including the country's own digital services exports, within the global digital economy. We applaud the Government of Pakistan's tireless efforts to create a comprehensive framework to protect the rights of data subjects. Further, we reiterate our support to work with the Government of Pakistan to ensure that the Draft Bill does not generate uncertainty and erect trade barriers that degrade the development and resiliency of Pakistan's digital economy.

We would like to express our appreciation for the extension of the deadline to submit comments on the Draft Pakistan Data Protection Bill dated August 25, 2021 and made available on the Ministry's website on August 27. We are pleased to provide the following comments and recommendations on key issues for your consideration.

- **Limit the Scope of "Sensitive Personal Data"**

We note that the Draft Bill has an expansive scope of sensitive personal data that includes financial information, physical identifiable location, travelling details, IP addresses and pictorial or graphical still or motion forms. The reason for inclusions is unclear and this will likely pose challenges in implementation without providing

meaningful benefit to data subjects, while severely impacting the ability of companies to provide services requested by the user or identify the user. Sensitive personal data should be defined in accordance with international approaches to promote and enable interoperability, expand international commerce, and advance Pakistan's digital transformation journey.

Recommendation: We recommend that the Government of Pakistan remove financial information, usernames, passwords, physical identifiable location, travelling details, pictorial or graphical still and motion forms, IP address and online identifier from the definition of sensitive personal data under Section 1.2 in line with international norms such as the General Data Protection Regulation (GDPR). For example, financial information is not covered as sensitive personal data in GDPR and in many jurisdictions, is covered under regulations within the banking sector instead. Otherwise, organizations in Pakistan will face limited grounds for collecting and processing personal financial information, putting them at a disadvantage with competitors in foreign markets, where it is treated more flexibly, as personal information.

- **Limit the Scope of "Critical Personal Data"**

As written, the definition of critical personal data in the Draft Bill under Section 1.2 d) "data relating to public service providers, unregulated e-commerce transactions and any data related to international obligations" - is broad enough to encompass non-personal data, i.e., information that relates directly or indirectly to a data subject. Legislation on personal data protection should only apply to personal data.

Phrases like "unregulated e-commerce transactions" and "data related to international obligations" are wide, vague, and unclear. In particular, the inclusion of "unregulated e-commerce transactions" within the definition of "critical personal data" has no international precedent. This definition, when read with the restrictions on cross border transfer and the requirement to process "critical personal data" only in Pakistan, creates an extremely onerous requirement.

Similarly, the inclusion of data relating to "public service provider" in the definition of critical personal data is a serious concern. Public service provider is defined as "any entity dealing and having personal data working under the government." It is a broad and vague term incapable of a precise definition, thereby leaving room for constant interpretational challenges.

Moreover, this new definition does not identify specific subsets of data, instead classifying data as critical personal data depending on how the data is used, for example, if the data is related to an "unregulated e-commerce transaction." This would require data processors to monitor data subjects and assess how they use their personal data to determine whether it is critical personal data or not, undermining the very premise of data protection and privacy.

Recommendation: We urge the Government of Pakistan to limit the scope of the Draft Bill to personal data protection and remove the treatment of non-personal and government data from this bill. Further, we urge that the Bill identify specific subsets of critical personal data, so that data processors do not have to react to a fluid definition, nor surveil how data subjects use their data.

- **Limit the Scope of the Extraterritoriality Provision**

We are concerned that the Draft Bill's extraterritorial application based on Section 3 is too wide and vague. The wording under Section 3.1 b) - "digitally or non-digitally operational in Pakistan" - makes it unclear whether the bill would bring within its scope even foreign companies that neither operate in Pakistan nor process data collected in Pakistan. Moreover, Section 3.1 d) that provides that the Bill applies to "any data subject present in Pakistan," raises the question whether even international visitors in Pakistan are subject to the provisions.

Normally, international companies are subject to laws of their own jurisdiction or laws having international application like GDPR. The extraterritoriality provision of the Draft Bill is wider than the EU GDPR and might result in companies geo-blocking Pakistani users. The Draft Bill should be applicable to the extent that such companies are collecting personal data from data subject in Pakistan during such commercial activities.

Recommendation: We recommend limiting the applicability of Section 3.1 b) to "services offered to the residents in Pakistan," and to limit the scope of Section 3.1 d) to "residents of Pakistan."

- **Limit the Consent Requirement for All Data Processing**

The Draft Bill imposes onerous requirements for processing all personal data, including under Section 5.1, the requirement to obtain a "separate consent shall be obtained from the data subject for each purpose." Such requirements on consumers are unlikely to have any meaningful benefit in terms of additional data protection.

Rather, because personal data is usually processed for multiple purposes, requiring separate consents for each purpose will likely result in a flood of consent notices that create 'consent fatigue' among users and overburden companies with a bureaucratic requirement that will disrupt the smooth functioning of Pakistan's digital economy.

Recommendation: We urge that the Government of Pakistan delete the sentence "a separate consent shall be obtained from the data subject for each purpose" and at the least, restrict consent requirements to new purposes of processing and to sensitive personal data rather than all personal data.

- **Commit to the Free Flow of Data**

The Draft Bill continues to impose restrictions on cross-border transfer of data. We are particularly concerned that the current draft language does not explicitly provide cases where data may be transferred and leaves it to the discretion of the Commission to devise a framework for cross-border data transfers in general.

Because the Draft Bill does not detail any principles or guidelines for the formulation of the proposed framework, there is effectively a restriction on the cross-border transfer of all personal data until the Commission formulates the necessary framework and conducts equivalency assessment. Even after the Commission formulates a framework for cross-border transfer, Section 15.2 requires that some undefined components of sensitive personal data be kept in Pakistan if it relates to public order or security, without clarifying the benefit envisaged from requiring local data storage for this data set. It also does not state who will be responsible for determining whether a restriction is necessary for public order or national security, or what the criteria are for designating data that relates to "public order" or "national security," which by themselves are broad terms and not defined in the Draft Bill. Because the qualifier does not identify fixed categories, Section 15.2 remains vague and can effectively be a blanket restriction on the cross-border transfer of all sensitive personal data.

Recommendation: We urge the Government of Pakistan to allow personal data to be transferred outside of Pakistan - with the consent of the data subject in the case of sensitive personal data. Additionally, we recommend a non-prescriptive and principle-based adequacy framework to add clarity on cross-border data flows. Preferably, the Personal Data Protection Bill should include details of framework and any specific requirements or approved mechanisms for the transfer of personal data, such as use of standard contractual clauses or binding corporate rules.

The ability to move data and access information across borders is essential for enterprises of all sizes to make day-to-day international commerce possible in the digital age. Cross-border data flows help economies thrive and present opportunities in every industry ranging from energy, digital, financial services, healthcare, manufacturing, and transportation. Sharing and analyzing data across borders delivers insights and services that benefit government, consumers, and businesses. When governments restrict data flows, they may impact the potential for innovative growth and undermine data security and fraud prevention, both of which rely on access to global data and redundancies/data storage in multiple locations.

- **Remove Data Localization Requirements**

The Draft Bill contains data localization measures including requirements under Section 14.2 that "Critical personal data only be processed in a server or data centre located in Pakistan" and under Section 15.2 that "the Commission devise a mechanism for keeping some components of sensitive personal data in Pakistan." Since the transfer of personal data is already proposed to meet strict requirements, the government can meet its sovereign objectives (e.g., security of citizen's data) without having to mandate any local storage requirements. Requiring specialized types of processing for different types of data categories often stored in the same account could create privacy risks by requiring companies to sort and identify the data that fall into this category to meet these additional requirements - not to mention, most service providers do not have systems to isolate critical personal data from other general account data.

Recommendation: We urge the Government of Pakistan to remove all data localization requirements in the Draft Bill. It is an ill-advised policy, as it presents a barrier to international trade and investment and will likely degrade the security of Pakistani citizen's data.

Localization creates a single point of failure, leaving systems more vulnerable to fraud and cyber threats. Forced data localization policies limit and hinder capabilities to tackle cross border financial crime such as money laundering and financing terrorism.

Localization obligations would make it difficult for growing businesses in Pakistan to compete in global markets. For example, it would make it difficult for companies to gain access to innovative technologies that depend upon cross border data flows such as data analytics, artificial intelligence, or machine learning. Local companies may also lose access to cost-efficient cloud services in the global market and incur substantial costs to operate, maintain additional servers, and increase processing and additional measures to ensure that their data is accurate, secure, and up to date.

Finally, data localization would prevent certain companies from offering services to Pakistani consumers, leaving them with less choice. This requirement can create a gap between the availability of hosting services and the required security capabilities regarding the risks posed by the processing of personal data, leaving companies without a compliant option to operate.

- **Clarify the "General Protected Rights" and Align with International Rules**

Under Section 28, the Draft Bill seeks to introduce a new data portability right and a new right not to be subject to a decision based solely on automated processing, including profiling. However, the Draft Bill lacks the necessary specifics of what these rights entail and how organizations can help give effect to these rights. For example, it lacks clarity on what data is portable and whether a data subject can object to any automated decision-making, even if it benefits them. There is also a question of how a process can be scalable without minor or harmless ways of automated decision-making. Such confusion and lack of clarity would hinder rather than help efforts to strengthen the rights of data subjects, since there are no concrete details to guide the implementation of these rights.

Recommendation: We recommend that the Draft Bill include further provisions, especially in a way that aligns the rights of data subjects with those under international rules. GDPR Article 20 can be used as a reference for the implementation of the data portability right, whilst GDPR Article 22 can be referred to in relation to the automated processing right.

Further, the data portability right under Section 28.a of the Draft Bill requires detailed provisions setting out the process and mechanisms for transfers of personal data at the request of a data subject, as well as any system of accreditation for requesters or recipients of such data. Meanwhile, Section 28.b should clarify that the right applies to profiling that leads to legal effects concerning the data subject, or similarly affects the data subject. Profiling that is part of the service requested by the data subject and which does not cause any legal or similar impacts to the data subject should be permissible.

- **Place adequate guardrails for the Commission**

Powers of the Commission under Section 34 of the Draft Bill are extremely broad and run the risk of adding legal requirements that will be unexpected by controllers and are beyond the scope of requirements set forth in the law. The Commission retains legislative, regulatory, judicial and law enforcement power, including legislating

frameworks for cross-border data flow, prescribing security standards, imposing "special measures for compliance" for large data processors, imposing fines, exercising search and seizure powers, summoning witnesses, adjudicating complaints, even reviewing its own decisions. Such broad powers, coupled with the absence of an oversight mechanism, lack appropriate safeguards, such as public consultation and measures to ensure that the companies subject to the Data Protection Act agree to any additional measures.

Recommendation: We recommend protecting the independence of the Commission and not assigning broad power and discretion to create entirely separate regulatory frameworks that are not clearly outlined in the Draft Bill. Rather, there should be additional scoping of expectations in the Bill itself to avoid unintended consequences. For instance, the Draft Bill should elaborate on the criteria that the Commission will use to determine whether a controller needs to comply with additional measures. Compliance measures should be explicitly stipulated in this Bill rather than specifying additional measures for controllers or processors. The Bill should also provide clarity on whether "big/large" in the context of controllers refers to the turnover of the data controller or the volume of personal data processed.

- **Commit to Regular and Transparent Dialogue with Business Community:**

It is critical that the Government mobilize relevant stakeholders to ensure that effective, transparent, accountable, and consultative regulatory processes are put in place. A long-term commitment to a transparent dialogue helps ensure that Pakistan's future data protection regime does not result in unintended consequences for the country's economy and digital transformation.

Recommendation: We recommend including a commitment for the Commission under Section 34 to consult with relevant stakeholders prior to issuing any compliance frameworks or guidelines. This includes providing appropriate time for submission of comments and establishing a consultative process for engagement with industry and relevant stakeholders in the formulation of compliance guidelines and implementation of the Bill.

- **Limit the Penalty to Corporate Liability**

It is unclear whether the fines detailed in Sections 44 and 45 would apply to individuals in their personal capacity or would be imposed on the data controller or processor by which they are employed, in addition to corporate liability under Section 47. This may amount to dual liability for the same offence and can be unreasonably onerous.

Recommendation: We recommend that the penalty be limited to the fine to be imposed on the entity, rather than on the individual employee. Most laws do not impose individual penalties or sanctions except for willful breaches or gross negligence.

***

The Chamber and USPBC appreciate the opportunity to voice our concerns about the latest draft of the PDPB. If you have any questions regarding our submission or need more information, please do not hesitate to contact Esperanza Jelalian, President of the U.S.-Pakistan Business Council, at ejelalian@uschamber.com and Abel Torres, Senior Director at the Center for Global Regulatory Cooperation, at atorres@uschamber.com.

.