

**Asia Internet Coalition (AIC) Industry Submission on Cambodia's Draft Law on
Personal Data Protection**

05 October 2023

To

H.E. Mr. Vandeth Chea
Minister of Post and Telecommunications
Ministry of Post and Telecommunication (MPTC), Government of Cambodia

The [Asia Internet Coalition](#) (AIC) and its members express our sincere gratitude to the Ministry of Post and Telecommunication (MPTC) and the Government of Cambodia for the opportunity to submit industry comments on **Cambodia's Draft Law on Personal Data Protection ("Draft Law")**.

The AIC is an industry association of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our member companies would like to assure the Ministry that they will continue to actively contribute to the security of digital platforms, products and services in support of the digital economy goals of Cambodia.

We are concerned that the Draft Law, in its current form, may impact many personal data processors and may lead them to limit their services in Cambodia. This can potentially result in unintended negative consequences for consumer choice in Cambodia and its digital economy.

As responsible stakeholders in this policy formulation process, we would greatly appreciate the opportunity to share our detailed comments and recommendations - in the section below - on the Draft Law, which we would like to respectfully request MPTC to consider.

We will also be grateful to the MPTC and the Government of Cambodia to uphold a multi-stakeholder consultation with the industry and look forward to offering our inputs and insights, directly through meetings and discussions to help shape an effective Data Protection Framework in Cambodia.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Thank you for your time and consideration.

Sincerely,



Jeff Paine
Managing Director
Asia Internet Coalition

Detailed Comments and Recommendations

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលម្អ Proposed changes in the text for Improvement
Article 22. Transfer of Personal Data Outside the Kingdom of Cambodia. A data controller may not transfer personal data to any country or territory outside the Kingdom of Cambodia unless authorized under this law and relevant legal instruments. Conditions, formalities, and procedures for transferring personal data outside the Kingdom of Cambodia shall be determined by prakas issued by the Minister of MPTC.	The free movement of data across borders is vital to Cambodia's economy and supports the best outcomes for Cambodian businesses and citizens. We therefore strongly recommend that the PDP Law does not restrict cross-border transfers of personal data collected in Cambodia. Enabling cross-border data transfers protects consumers by allowing businesses to implement best practices for data privacy and security, such as decentralized cloud data storage solutions and shared systems that are resilient to outages from malfunctions or natural disasters, and unauthorized access by third parties. Cross-border data transfers will also lower barriers to international trade and investment in the Cambodian economy by reducing compliance costs.	A data controller may not transfer personal data to any country or territory outside the Kingdom of Cambodia ~~unless authorized under this law and relevant legal instruments.~~ ~~Conditions, formalities, and procedures for transferring personal data outside the Kingdom of Cambodia shall be determined by prakas issued by the Minister of MPTC.~~

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលម្អ Proposed changes in the text for Improvement
	The World Bank notes that free and open cross-border data flows are key to the global trade in digital services, and offers meaningful opportunities for developing countries to benefit from the massive growth of the global digital economy sector. They also note the presence of multiple studies that confirm that data localisation will have alarming negative consequences for national GDP growth and foreign investments. For instance, the European Centre for International Political Economy estimated that omnibus data localisation will result in GDP decline, loss of jobs and investments, and disruption of supply chains. Cross-border transfers will reduce operating costs of Cambodian businesses and prices for local consumers, and enable industries across all economic sectors to benefit from global data flows since nearly every aspect of the modern economy employs digital technologies and communications tools. According to the World Bank, after two decades of rapid growth, Cambodia's next wave of growth will come from the digital economy. In 2021, the Supreme National	

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលម្អ Proposed changes in the text for Improvement
	Economic Council noted that for Cambodia to benefit from digital economy growth, the country needed an enabling legal and regulatory framework. The World Bank echoed these concerns, calling specifically for a data protection regime that would encourage businesses and service providers. It is therefore critical for Cambodia's PDP Law to foster the digital economy by removing artificial barriers to cross-border data flows.	
Article 24. Location of Personal Data Storage. A data controller shall store collected personal data in the Kingdom of Cambodia. A data controller may store personal data in its own personal data storage system or a data center or a secure cloud system of a third party licensed by MPTC in accordance with other laws and regulations in force. Technical specifications, conditions, and rules for managing data centers or secure cloud systems for storing personal data shall be determined by	Mandating the storage of personal data in Cambodia has the same effect as Article 22, which prohibits external transfers of personal data. This is problematic for the reasons explained above. The economic consequences of data localisation mandates are severe. According to ITIE, econometric modeling using a point-scale based on OECD market regulation data showed that over five years, for each point that regulations restrict cross border data flows, a country's gross trade output is reduced by 7%, it's productivity drops by 2.9%, and downstream prices rise by 1.5%.	~~A data controller shall store collected personal data in the Kingdom of Cambodia.~~ ~~A data controller may store personal data in its own personal data storage system or a data center or a secure cloud system of a third party licensed by MPTC in accordance with other laws and regulations in force.~~ ~~Technical specifications, conditions, and rules for managing data centers or secure cloud systems for storing personal data shall be determined by prakas issued by the Minister of MPTC.~~

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលម្អ Proposed changes in the text for Improvement
prakas issued by the Minister of MPTC.	Another econometric modeling study by McKinsey has shown that increased cross-border data flows grew global GDP by 10% -- \$2.8 trillion -- in 2014, with emerging digital markets standing to benefit from 50% GDP growth by embracing cross-border data flows. Those potential economic gains have grown many times over as the amount of data that transits global networks has since multiplied exponentially. Multinationals looking to invest may forgo Cambodia in favor of markets with less burdensome costs of entry. The US National Trade Estimate identified restrictions on data flows and data localisation requirements as a leading impediment to foreign direct investment by US companies. Undue restrictions on data flows will also artificially limit the ability of local 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 and stifling innovation.	
Article 16. Protection of Special Categories of Personal Data.	Since special categories of personal data (SCD) attract additional obligations, it is critical	Data controllers and data processors must <i>obtain consent for the processing of</i> ~~provide~~

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលម្អ Proposed changes in the text for Improvement
Data controllers and data processors must provide special protection to special categories of personal data in accordance with legal instruments in force. Special categories of personal data protected under this law includes, but is not limited to, biometric data, genetic data, health data, and data related to ethnicity and religion. The list and conditions of special categories of personal data and special protections for special categories of personal data shall be determined by prakas issued by the Minister of MPTC.	that the PDP Law clearly and exhaustively defines the types of data that are covered by this requirement. Globally, laws that prescribe additional obligations for SCD exhaustively list the SCD so as to not create uncertainty and unpredictability for both domestic businesses and foreign investors. Unfortunately, the PDP Law uses the phrase “includes but is not limited to”, which generates significant uncertainty for data controllers who are unable to plan their compliance as long as executive authorities have open-ended powers to designate any data type as SCD. Moreover, the term “special protection” is vague and undefined, which leaves data controllers unclear about their compliance obligations. We recommend that: • In line with global best norms, the restrictions on processing SCD should only include information that poses a higher risk to individual privacy because of its inherent nature.	~~special protection to special categories of personal data in accordance with legal instruments in force.~~ Special categories of personal data protected under this law ~~are includes, but is not limited to,~~ biometric data, genetic data, health data, and data related to ethnicity and religion. ~~The list and conditions of special categories of personal data and special protections for special categories of personal data shall be determined by prakas issued by the Minister of MPTC.~~

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលម្អ Proposed changes in the text for Improvement
	• There should be an exhaustive and precise list of SCD in the PDP Law. • No additions to the SCD list should be possible by executive authorities such as MPTC. • The term “special protection” is replaced with an understandable description of the obligations and prohibitions that data controllers will face in respect of SCD.	
Article 7. Age Conditions for Collection, Use, and Disclosure of Personal Data. Consent to the collection, use, or disclosure of personal data mentioned in Article 6 of this law only applies to natural persons who are at least 15 years old. If a natural person is less than 15 years old, the collection, use, or disclosure of his or her personal data is only lawful upon the consent or approval of the parent or guardian. A data controller must examine and verify each case of consent or approval purported to be given by the	In line with global best practices, the age of a child for the purposes of a data protection law should be 13 years of age. This aligns with the US Children’s Online Privacy Protection Act (“COPPA”), the EU GDPR and guidelines under Singapore’s Personal Data Protection Act (“PDPA”). By barring adolescents under the age of 15 from validly consenting to digital services, there is a risk of locking young adults out of the digital economy. This would even prevent them from accessing useful online information such as educational resources. We recommend that data controllers should be required to take reasonable steps to verify age but that the law should not prescribe specific	We recommend replacing references to “15 years old” with “13 years old” throughout Article 7.

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលម្អ Proposed changes in the text for Improvement
parent or guardian of the data subject who is less than 15 years old.	age verification mechanisms. No single method of age verification mechanism can achieve 100% accuracy and prescribed methods may unduly increase costs and negatively impact a consumer's experience without actually protecting the child. Additionally, imposing prescriptive age verification, parental consent mechanisms or processes and broad child-related data processing prohibitions could be unduly prohibitive and may not be appropriate to the specific circumstances of data collection or processing. For example, if certain technological measures must be implemented, these may be onerous for smaller businesses that target children (e.g. local toy stores or educational websites) and may stifle innovation by smaller, local companies in Cambodia. It is important to also note that parental consent does not in itself prevent exposure to harmful content online; in practice, this is achieved through the implementation of special protections. Instead of having the PDP Law impose age verification, parental consent requirements and child-related data processing prohibitions, the better approach may be for the industry to work with the MPTC in	

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលម្អ Proposed changes in the text for Improvement
	preparing Codes of Practice around verification processes. As industry standards evolve and become more robust, so can the Code of Practice. Given that verification mechanisms are technical and industry best practices around it evolve constantly, it is important to adopt a co-regulatory, multi-stakeholder approach to find the right solution to this.	
Article 17. Unlawful Data Practice. Data controllers are strictly prohibited from engaging in any of the following practices: (a) charge an extra fee or raise the price for a good, service, or feature when a data subject exercises any right under this law; (b) terminate, refuse to provide, or degrade goods or services to, or otherwise retaliate against a data subject that exercises any right under this law;	We agree that it is important that data controllers are not able to retaliate against data subjects who exercise their data subject rights by, for example, charging unreasonably high fees to access personal data held by a controller. However, we think there is a risk that the current drafting of Article 17 goes well beyond preventing retaliation by data controllers and would prevent reasonable, commercial activities. First, data controllers should be able to charge reasonable fees to cover the administrative costs of compliance with a data subject right.	We recommend three changes: Article 17. Unlawful Data Practice. Data controllers are strictly prohibited from engaging in any of the following practices: (a) unreasonably charge an extra fee or raise the price for a good, service, or feature when a data subject exercises any right under Chapter 8 of this law; (b) unreasonably terminate, refuse to provide, or degrade goods or services to, or otherwise retaliate against a data subject that exercises any right under Chapter 8 of this law;

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលម្អ Proposed changes in the text for Improvement
	Secondly, there may be instances where it is not possible to continue offering a service to a consumer if they have exercised a data subject right. For example, if a data controller is relying on legitimate interests as the legal basis to process data and an individual objects to this processing, it may be necessary for the data controller to terminate services to this individual as it will no longer have a legal basis under the Act to continue to provide services. On this basis, Article 17 should be clarified so that the prohibition only applies to unreasonable activities.	