24 August 2022

To
Mr. Zunaid Ahmed Palak
Minister of State, Information, Communication and Technology Division
Ministry of Posts, Telecommunications and Information Technology
People's Republic of Bangladesh
Dhaka, Bangladesh

Subject: Industry submission by Asia Internet Coalition on the draft Data Protection Act 2022 (July draft)

Dear [Minister Palak]

On behalf of the Asia Internet Coalition ("**AIC**") and its members, I am writing to express our sincere gratitude to the [Ministry of Posts, Telecommunications and Information Technology ("**MOPTIT**")] for the opportunity to submit comments on the draft Data Protection Act 2022 dated 16 July 2022 ("**Draft Act**"). AIC is an industry association comprising leading internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of internet and ICT policy issues.

Data-driven innovation is powering the growth of Bangladesh's emerging digital economy, creating opportunities for both established companies and new entrants, and giving people access to better products and services. At the same time, it is important that people have confidence that their personal data will be protected. In light of this, we commend the efforts of the Bangladesh government to enhance the protection of data in Bangladesh through the Draft Act.

Such efforts are critical, particularly at a time when the Covid-19 pandemic has resulted in a great deal of our lives moving online, underscoring the importance of innovation, digital adoption, digital security and privacy. It is more critical than ever to protect personal data particularly when economies and companies are transitioning rapidly into the digital space.

Through our work with regulators in jurisdictions around the world on best practices in legal and policy frameworks for privacy, we have seen that the most successful data-driven regulations balance both the objective of protecting consumers' personal data with that of ensuring the country benefits from the opportunities created by the wave of data-driven services, technologies and innovation. While we believe that many aspects of the Draft Act go some way towards these dual objectives, we also believe that there are several provisions that require further consideration to bring it in line with international good practices. This is especially important to allow Bangladeshi businesses to participate and flourish in the global economy, as well as to promote international investment in Bangladesh's digital economy.

We believe that the Draft Act should be developed in a balanced manner, which accounts for diverse social, economic, and innovation-oriented objectives. It should protect the rights of people but also not be drafted in an overbroad manner that could result in roadblocks to innovation and technological advancement in Bangladesh. **As such, our comments are aimed at refining the Draft Act to create a framework which aligns more closely with international best practices and allows participants in the Bangladesh economy to flourish on the global stage.**

As responsible stakeholders, we appreciate the ability to participate in this discussion and the opportunity to provide input into the policy-making process. Please find below our detailed comments and recommendations, which we respectfully request you to consider.

A. COMMENTS AND RECOMMENDATIONS

Firstly, there are several items in the Draft Act that we commend and support as they are now more aligned with international benchmarks such as the European Union's General Data Protection Regulation ("**GDPR**"), Singapore's Personal Data Protection Act ("**PDPA**"), the APEC Privacy Framework and the OECD Privacy Principles (together, the "**International Benchmarks**"), than in previous versions of the draft Act, achieving a better balance between privacy concerns and the need to foster innovation. For example, we support the various, equally weighted lawful bases of processing personal data that are available to organisations in section 7. We also support the approach to consent articulated in section 7, the recognition of the accountability principle (that the data controller is primarily responsible for the processing by a data processor) in sections 21 and 24, and the balanced data breach notification requirements in section 28.

However, we set out below our top recommendations to bring the Draft Act more in line with international best practices to help Bangladesh achieve its digital economy goals whilst still protecting individual privacy.

1. **<u>Scope of application</u>: The Draft Act should make clearer that it only applies to data that directly or indirectly identifies an individual.**

   Unlike an earlier draft of the Personal Data Protection Act issued in 2020 ("**2020 Draft**"), we note that this Draft Act has replaced all references to "personal data" with just "data". "Data" is also defined in section 2(c) as meaning "a representation of any information, knowledge, fact, concepts or instructions which are being prepared or have been prepared in a formalized manner and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and may be in any form including computer printout, magnetic or optical storage media, punch cards, punched tapes or stored internally in the memory of the computer, and includes the personal data for that purpose", which is broader than the 2020 Draft's definition of "personal data" which was limited to information that could directly or indirectly identify an individual. Whilst the latest version of the Draft Act does include a proviso in that same section that "*anonymized, encrypted or pseudonymized data which is incapable of identifying an individual shall not be included within the purview of personal data",* the legislative impact of this is limited since "data" rather than "personal data" is used throughout the Draft Act. It is unclear if this may be a translation issue. Nevertheless, we note that section 4(2) clarifies that the Draft Act does not apply to "anonymised, encrypted or pseudonymized data". The Draft Act should make clear that it only applies to data that directly or indirectly identifies an individual under scope of application in Section 4(2).

   Effective privacy laws are meant to protect an individual's privacy. Mishandling personal data could have a big impact on an individual's life. This is why privacy laws are created – to protect personal data. Hence, we recommend that the Draft Act make clear that it only applies to data that can identify an individual. Data that cannot identify an individual is of much lower risk to an individual's privacy since it cannot be linked to a human person. Furthermore, such non-personally identifiable information is especially important to companies who analyse large amounts of data to improve their products, operations and customer service. For example, self-driving systems often need to process huge amounts of data, including anonymized driving and

traffic patterns, to improve their safety algorithms. Imposing additional protections on this type of data does not significantly benefit individual privacy (since it does not identify the person) but could restrict the ability of businesses to innovate and compete effectively in the modern, digital economy.

Therefore, we recommend reinstating the defined term of "personal data" and using this instead throughout the Draft Act to make clear that protecting personal data is the main focus. Reference can be taken from the GDPR in crafting the definition of "personal data" to ensure that it is aligned with International Benchmarks.

2. **<u>Commencement date</u>: The Draft Act should expressly provide in section 1(2) for a two-year grace period for compliance from the date it is published in the Gazette.**

Section 1(2) mentions that the Draft Act will come into force on the date notified by the Government. We understand that this effective date could be immediately once the statute is enacted. An immediate effective date would be detrimental for companies, such as our members and even smaller businesses, who wish to be compliant. Organisations generally need time to get their processes and internal policies in order, upgrade their systems and provide training to their employees. If the Draft Act comes into effect immediately this will result in widespread instances of technical breaches. A clearly defined grace period will allow predictability and certainty for companies.

We do agree with the principle behind the newly included section 1(3) which contemplates staggered commencement dates for different sections so that organisations presumably are granted more time to comply with the more complex requirements under the Draft Act. Nevertheless, we still consider that the actual staggered grace periods should be clearly defined for greater certainty.

3. **<u>Territorial application</u>: The extra-territorial application of the Draft Act in sections 4(b) and (c) should be removed, or else should have further clarifications such as those in Recital 23 GDPR.**

As currently drafted, the Draft Act applies to: (a) those within Bangladesh who collect and process data; (b) those outside Bangladesh who collect and process data of Bangladesh citizens anywhere in the world; and (b) those outside Bangladesh who process data in connection with any commercial delivery of goods or services in Bangladesh or the profiling of data subjects anywhere. This means that the obligations of the Draft Act apply irrespective of the purpose of that processing (i.e. even if it is incidental) and irrespective of whether the service has any relation to Bangladesh (since it would apply to businesses that have a single overseas Bangladesh citizen as a customer). This extra-territorial application may have the unintended effect of causing non-Bangladesh based companies to geo-block some or all of their services and resources so that they will not be accessible to Bangladeshi users, as a precautionary measure to avoid inadvertently infringing the law. This will result in fewer benefits and choices to individuals in Bangladesh.

Nevertheless, we understand that there are occasions where it is necessary for extra-territoriality to apply. For example, where an offshore company *unambiguously* targets the Bangladeshi market and this is evident from the use of Bengali or the display of currency in Taka, it may be relevant for such company to be subject to the rules of the Draft Act. The Draft Act should more clearly articulate these situations in section 4(c). Inspiration can be taken from Recital 23 of the

GDPR which mentions that factors such as the use of a language or a currency generally used in the jurisdiction will be taken into consideration.

4. **<u>Legitimate interest legal basis</u>: We request adding a "legitimate interest" legal basis for processing in section 7.**

Section 7 outlines the legal bases for processing under the Draft Act, but it does not include the well-established legitimate interest basis for data processing featured in data protection regimes like the GDPR and the PDPA. The legitimate interest legal basis is critical for businesses, which use it for a number of important purposes that are not expressly provided under the current language of the Draft Act, including the protection of internal systems from cybersecurity threats. For example, organisations use the legitimate interest basis for processing related to operations to guard against unauthorised access by bad actors, malware prevention, and the prevention and detection of security incidents.

To help align the Draft Act with international data protection standards and ensure that businesses can take steps to protect their customers from fraud and secure their internal operations, we recommend adding a legitimate interest legal basis for processing.

5. **<u>Rights of foreign data subjects</u>: We request that the "rights of foreign data subjects" in section 17 should be deleted.**

Section 17 is unusual and out of alignment with international benchmarks, as well as approaches to privacy laws elsewhere in the region, such as the draft India Personal Data Protection Bill. Section 17 creates considerable uncertainty in respect of the obligations data controllers in Bangladesh would have to comply with, as it appears to impose obligations arising under the laws of other jurisdictions. We recommend that this Section be deleted from the Draft Act.

To the extent that the objective of the clause is in relation to granting the same data subject rights or access, correction, portability and erasure to a non-citizen, emphasise that the scope of the Draft Act in section 4(1)(a) already applies the same rights to non-citizens residing or located in Bangladesh and this section 17 does not add much value.

6. **<u>Cross-border transfers</u>: The data localisation provisions in respect of sensitive data, user generated data and classified data in section 42 should be deleted, as should the requirement "to meet his necessity" for consent of the data subject in section 43(2)(a) and the exception in section 43(2)(b) that permits cross-border transfers for the "purpose of maintaining international relations, cross-border business, immigration or any other data as specific by the Government, from time to time" should be aligned instead with International Benchmarks.**

All privacy frameworks should be built on common principles -- giving people rights over their information, ensuring companies implement strong privacy practices, and holding them accountable when they don't. It is essential that these frameworks facilitate the free flow of data across borders clearly. The provisions of sections 42 and 43 are too restrictive and vague on the requirements around cross-border data transfers.

We commend the inclusion of the additional grounds on which data is permitted to be transferred cross-border (as opposed to the previous April 2022 version of the draft Act which only permitted this with data subject consent). However, the exceptions here are vague and unclear. For

example, if an international non-profit or charitable organisation wanted to transfer data out of Bangladesh to facilitate a scholarship or a donation, would this be permitted under the "cross-border business" exception, notwithstanding that the purposes are not commercial in nature? Further, there is no guidance on what would be considered "consent to meet his necessity" for a cross-border data transfer.

We recommend reinstating the first option from the 2020 Draft which permitted cross-border transfers to white-listed territories and in certain prescribed circumstances, including where necessary for the performance of a contract between the data subject and the data controller. This would align with International Benchmarks and provides some practical flexibility for cross-border transfers that still ensures that there are safeguards for the data. The exceptions from the 2020 Draft, including public interest and vital interests, are also aligned with those under Article 49 GDPR. The legal bases for transfers should also be expanded to include the possibility of approved contractual clauses, an international treaty or trade agreement to which Bangladesh is a party, intra-group schemes approved by the government, and where transfers are necessary for the provision of services. From a privacy protection perspective, it would be more effective to impose an obligation on the relevant organisation to ensure that the overseas recipients provide a standard of protection equivalent to that under the Draft Act instead.

Decisions about where to store data should be based on technical considerations of the global internet and our users' needs. This is the best way to ensure strong performance, reliability, and security. Because of how the global internet was built and has evolved, data is physically transferred across international borders as part of almost every online communication or activity, often including those which are wholly domestic and where there is no change in data controller or data processor so the same laws and policies apply. The internet was built to be a decentralised patchwork of tens of thousands of different networks that connect and communicate with one another by using standard technical protocols. Each of these networks routes data around the globe. The networks are generally agnostic of the physical "journey" of the data and instead optimise routing in real time to reduce latency and increase network resilience. Laws should permit or promote cross-border data transfers, rather than prohibit or restrict them. Insofar as laws do govern cross-border data transfers, the laws should be narrowly tailored so that they apply only to legal data transfers between data controllers or data processors and ensure any preconditions that must be met before data is transferred are not so burdensome as to result in data localization. Therefore, the language regulating the "cross-border data transfer" or transfer "to a place or system outside Bangladesh," in Articles 38 and 42 is infeasible, if not impossible to accomplish, and should be revised to reflect the reality of international data flows. We recommend Articles 38 and 42 be narrowed to clarify that this is in reference to the transfer of data between two or more data controllers or data processors where at least one of the data controllers or data processors is based in a jurisdiction other than Bangladesh.

While we agree with the intent to deliver secure services for the citizens of Bangladesh, policies that inhibit or restrict cross-border data transfers will in fact make Bangladeshi users' data less secure. Requiring default data localisation for sensitive data, classified data and user-generated data would cut off Bangladesh from accessing state-of-the-art cloud security enterprises and implementing best practices designed to keep user data secure. The infrastructure of the internet – both physical and software – work as a whole system to allow companies to serve billions of users with real-time conversations and experiences. Companies that facilitate cross-border data transfer host their websites, apps, products, and services, and process user data across data centres located around the world. That means that user data is distributed across various servers globally — irrespective of the geographic origin of any data. These global data centres are the

foundation of the global infrastructure of the internet, and being able to transfer data internationally, and store it in these data centres, not only allows companies to increase the resilience of our services in the event of a network disruption such as natural disaster or power outage, it also helps us keep our global community safe by decentralising data and thus making it less vulnerable to malicious actors. These data centres are also supported by a much larger network of local infrastructure in the regions and countries, which enables content to be cached locally in order to reduce latency and improve users' experience. Moreover, malicious third parties can often be domestic actors, which means that storing data within a single jurisdiction may exacerbate security concerns instead of resolving them. Cross-border data flows are critical to following best practices for data privacy and security. Further, after incurring significant up front investments in the necessary infrastructure required for compliance, companies of all sizes are often unable to bear the additional costs to update their data management systems regularly. This would put them at greater risk of being targeted by cybercriminals for data breaches and ransomware attacks.

Furthermore, it is unclear why there is a distinction made for user-generated data to be stored in Bangladesh by default under section 42 – such data is unlikely to be particularly sensitive or vital to national security concerns. The definition of user-generated data is overly broad, and includes the undefined "personal data", which as suggested above, should be reinstated and crafted to align with International Benchmarks, such as GDPR. Additionally, there is no definition of what would be considered "classified data" other than that the government may designate "any data" as such. It is unclear if it is intended to mean government-held data or otherwise, and will cause confusion for businesses seeking to comply. The bill should provide a definition of an exhaustive list for the definition of "classified data" in order to provide clarity for controllers regarding what data is in scope.

In addition, the data localisation provision applies equally to both resident and non-resident companies. This means that companies, irrespective of their location or country of incorporation, will be required to store certain categories of data on servers and data centres located in Bangladesh. From a technical standpoint, this localisation requirement would require companies to systematically monitor and sift through all the user data (potentially all over the world) in order to identify the three categories of data and ensure these data are not transferred outside the country without meeting the statutory conditions. Such a requirement will be extremely expensive and operationally and technologically difficult, if not impossible, to implement for companies of all sizes – in particular SMEs who lack the resources or infrastructure to accomplish this.

The current data localisation provisions will also hamper the Bangladeshi economy. Due to the significantly increased compliance and regulatory costs, Bangladesh would become a less attractive destination for overseas investors and increase costs for local companies seeking to take advantage of cloud technologies. Furthermore, storing sensitive and user generated data in Bangladesh could cause latency in global online services for Bangladeshi internet users, resulting in such services becoming harder to use and access. These restrictions would be particularly problematic given that the reliance on digital services and technologies has only intensified during the COVID-19 pandemic.

Data localization requirements will also artificially limit the ability of companies, especially small and medium sized Bangladeshi businesses, by making it harder for Bangladeshi businesses to harness the value of the data, stifling innovation and economic growth, and reducing productivity. Econometric modelling 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%, its productivity drops by 2.9%, and downstream prices rise by 1.5%.[1] When governments impose data localization requirements on businesses that are based or operating within their borders, it stifles their potential for economic growth. This will be especially true for Bangladesh, which exported nearly $1 billion worth of ICT products in 2018 and is a major contributor to the growing national GDP that is projected to become the world's 24th largest economy by 2030. Independent analyses have found 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.[2] For Bangladesh to continue to grow its information technology sector and tech-dependent sectors in relation to global markets, cross-border data flows are a critical driver which must be encouraged and preserved.

7. **<u>Government access and requests for data:</u> Provisions regarding government access and requests for user data in Articles 10(2)(d), 36(2)(a)(i), (iv) and (v), 40 (1), 42(1), and 63(1) should be amended to align with international frameworks and avoid conflicts of law.**

   The provisions regarding government access to data from foreign based providers in Articles 10(2)(d), 36(2)(a)(i), (iv) and (v), 40, 42(1), and 63(1) are inconsistent with international frameworks and will create conflicts of law. The collective effect of these provisions is to create a framework for government access to data. This type of framework should best be dealt with in a separate legal instrument such as the Budapest Convention, as opposed to in a Data Protection Act which is meant to protect citizens' personal data.

   In Article 10(2)(d), the requirement that "any data" from a data subject which is "necessary for the prevention, detection, investigation of an offence or for the national security" may be collected by "another person or statutory body or government entity" is unclear, broad, may create conflicts of law, and is not aligned with international frameworks. "Any data" and "national security" are undefined in the draft bill, which may cause concern for businesses seeking to provide services or operate in Bangladesh.

   Articles 36(2)(a)(i), (iv) and (v) give broad authority to the Data Protection Office to access data for the purpose of examination or necessary for its functions. Similarly, insofar as the Articles regard user data, such functions are broadly defined, inconsistent with international frameworks, and will create conflicts of law.

   Article 40 provides that data controllers and data processors must "provide" information under the direction of the Director General. This provision is broad and it is not clear if "provide" means disclosure of user data or an investigation of business practices. If the requirement includes user data, such requirement should be revised to exclude user data as it is also broad and will create conflicts of law.

   The data localization provisions for sensitive data, user created or generated data, and classified data in Article 42(1) will not address the jurisdictional and conflict of law barriers that prevent foreign providers from producing data in response to direct requests from law enforcement. Regardless of where the data is stored, companies are subject to the law of the jurisdiction in

[1] https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

[2] https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.pdf

which they are incorporated, which place strict limits on their ability to disclose contents and most metadata, subject to certain exceptions. Further, the restrictions on the ability of foreign courts and law enforcement agencies to issue requests for the three classes of data in Article 42(1) are not aligned with international practices and create conflicts of law. This is because a foreign-based provider may still receive a compulsory demand from the jurisdiction where they are based for a Bangladeshi user's data, or targeting another user where a Bangladeshi users' data is inextricably linked to/included in the production. In these instances, this provision of the draft Data Protection Act could present providers with a possible conflict of law where they either have to produce data in response to the compulsory demand in spite of the draft Act's provision, or resist the compulsory production and potentially face criminal or civil noncompliance penalties in the jurisdiction where they are based.

Lastly, the powers of the government to issue directions to the Director General as it "may think necessary in the interest of the sovereignty and integrity of Bangladesh, the security of the State, [and] friendly relations with foreign States or public order" in Article 63(1) may create conflicts of law insofar as they require foreign providers to provide user data to the Bangladeshi government.

As stated above, U.S. companies are subject to U.S. law, which places strict limits on their ability to disclose contents and most metadata, subject to certain exceptions. This means that countries should request data through legal channels, such as the U.S. Mutual Legal Assistance Treaty (MLAT) process for U.S.-based providers (or using Letters Rogatory where no MLAT is in place) in order to avoid the aforementioned conflicts of law.

We recommend that Bangladesh consider signing an MLAT with the U.S., and acceding to the Budapest Convention in order to facilitate law enforcement requests for data from U.S.-based providers. In addition, Bangladesh should establish a single point of contact for government-to-government requests. This would ensure that requesting agencies are familiar with U.S. legal and constitutional requirements, and have reviewed requests to ensure they meet U.S. standards. It should also be noted that many U.S. companies have processes for responding to and granting disclosure requests, and that many such requests from Bangladesh have been previously granted.

8. **<u>Notice requirements</u>: Effort should be made to ensure the Rules referred to in section 8 do not impose prescriptive notice requirements to avoid notice fatigue whilst still maintaining transparency for consumers, and section 22 should be deleted to streamline the notice requirements.**

Section 8 mentions that the notice requirements will be prescribed in subsequent Rules. Prescriptive and detailed notice requirements should be avoided as they may result in notice-fatigue for data subjects if the volume of detail that must be provided to data subjects is overwhelming. We suggest that the notice requirements in the Rules should only include the types of personal data and purposes of processing and to allow organisations greater flexibility on how the notice should be presented. This would be consistent with the approach taken under Singapore's PDPA where data subject rights are balanced against a more streamlined user experience.

Furthermore, there is an overlap between the section 22 requirement for specific information to be provided and the notice requirement in section 8. We recommend deleting section 22 and combining the items listed with the Rules to be issued under section 8 so that all notice

requirements are consolidated. This will help to minimise confusion and lack of clarity in the Draft Act, particularly around what must be notified to data subjects.

9. **<u>Sensitive data</u>: The definition of Sensitive Data in section 2 (v) should be exhaustive, and "financial or commercial data" should not form part of Sensitive Data.**

Having an exhaustive definition of "sensitive data" would be aligned with that under International Benchmarks such as GDPR which typically do not include any powers for the regulator to further expand the list. Sensitive personal information should actually be more sensitive and of a higher risk to individual privacy. In this respect, we acknowledge that the list now *appears* to be narrower since "passwords", "caste or tribal custom" and "religious or political belief or opinion" have been removed. Nevertheless, the definition still permits further types of data to be prescribed as being sensitive data, so the effect of such edits is limited. Having a closed list will give organisations greater certainty over the types of data that are accorded the additional protections under the Draft Act.

Financial or commercial data is not classified as sensitive data in major data protection regimes, such as the EU's GDPR. In addition, not all types of "financial data" are always more sensitive to individual privacy. For example, a person's credit history may be more sensitive in certain circumstances, but the fact that he or she has opened a bank account with a particular bank may not be. "Commercial data" is not defined in the Draft Act. Its meaning is too vague and broad. It is important that the list of "sensitive data" is not overly broad as this would increase compliance costs for companies unnecessarily, which may divert resources away from innovation and investment and hamper overall economic growth.

10. **<u>Collection of data from a third party</u>: Section 10 should be deleted in its entirety, section 5(f) and section 23 should be amended to permit the collection, use and disclosure of personal data from third parties as long as it is compatible with the original purpose. This approach would balance individual privacy with business efficiency.**

Section 10(2) restricts the circumstances under which personal data may be collected from a third party (rather than directly from the data subject), both Section 5 (f) and Section 23 restrict the circumstances under which personal data may be disclosed. These are unusual requirements and not aligned with any International Benchmarks. Although there are exceptions to this rule, these are very limited and would unduly restrict the ability of organisations to exchange data for innovation and other services whilst still respecting the data subject's rights.

Under International Benchmarks such as GDPR and Singapore's PDPA, the collection of personal data from third parties is generally permitted subject to notice and other transparency requirements. The key is for the data subject to understand how their data will be processed, and a similar approach should be taken here. Unduly restricting the ability of organisations to collect data from third parties, particularly in the context of large global organisations that often share personal data amongst several entities in order to provide a seamless service for the benefit of the customer, would not be feasible. Such restrictions would also put local Bangladesh businesses at a disadvantage in taking advantage of the global digital economy as it would reduce their competitive advantage and ability to leverage data analytics (which typically requires the transfer and processing of large quantities of data) to offer better products and services both in Bangladesh and globally.

Where such collection, use and disclosure is for a purpose other than that which the personal data have been collected, and such processing is not based on the consent of the data subject, this should be permitted provided it is compatible with the purposes for which the personal data was originally collected.

11. <u>Data protection register</u>: The requirement to register all purposes for which data is collected or processed with the Director General in sections 44 and 45 should be deleted.

This is out-of-step with all other International Benchmarks and would have several negative effects. It is also unclear what is the intended data protection benefit that this requirement seeks to achieve.

Firstly, it would stifle any form of data innovation and business in Bangladesh given the onerous requirement to ensure that every single purpose of processing is registered with the Director General. This would discourage businesses from using data at all, which would stifle economic development and product innovation. Today's economy and technological developments are largely data-driven and rely on investments that utilise data in new ways to gain insights to deliver cutting-edge products and services to people. If every single purpose needs to be reported to a central authority, this will increase the cost of compliance for all companies including small local businesses and discourage people from using data at all.

Secondly, it would create a great administrative burden for the office of the Director General. As highlighted above, data is key to the modern economy, which means that effectively every single business collects and processes data, often in multiple ways for multiple purposes. Creating a centralised registry of these purposes would mean significant resources would be devoted just to maintain this record rather than on truly ensuring that the Director General is prioritising high priority regulatory activities such as dealing with data breaches.

Thirdly, this requirement when read with section 4 of the Draft Act may also cause companies to think twice about setting up or doing business in Bangladesh, and geo-block some or all of their services accessible to Bangladeshi users, since having a publicly accessible register containing confidential information poses a risk to user confidentiality and privacy as well as confidentiality of sensitive business information.

Lastly, registration does not necessary lead to meaningful compliance by organisations because even if offshore organisations do in fact register with local regulators, the practical challenges of enforcement against offshore entities still remains, together with the ongoing risk of organisations geo-blocking their services as highlighted above. In our experience, regulatory efforts in this regard are better spent raising public awareness on data subject rights, as we often find that the data subjects and consumers are one of the biggest factors in acting as a check on the compliance of such organisations through complaints and other consumer-initiated actions.

12. <u>Security requirements</u>: The power of the Director General to issue prescriptive security standards for the protection of personal data in section 24(1) should be removed.

While most, if not all, International Benchmarks require organisations to protect the personal data under their possession or control, issuing prescriptive standards will create onerous requirements and increase the cost of compliance for smaller local businesses, which may in turn stifle their ability to grow and innovate. Furthermore, prescriptive standards do not allow companies to keep up with the fast-evolving threat landscape as these standards may become obsolete very quickly.

Laws should be future-proof and technology-neutral and allow a degree of flexibility in appropriately achieving security of personal data. Therefore, organisations should be permitted some flexibility in deciding what measures are most appropriate to the type of processing that they are undertaking. The security measures required of a multinational data analytics company are not the same as those required for a local store with a mailing list. Inspiration can be taken from Singapore's PDPA which requires organisations to implement "reasonable" security measures.

13. **Data protection by design: The data protection by design obligations under section 32 should allow for greater flexibility in designing the measures to be implemented and prescriptive measures should be avoided.**

Inspiration can be taken from Article 25 GDPR which expressly allows data controllers to take into account factors such as "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing". Including these explicit factors and avoiding prescriptive requirements would help companies find the right solutions to implement which are appropriate to their business and risk. For example, the types of measures to be implemented for a large multi-national healthcare organisation would be very different from a small grocery store with a customer loyalty programme, and therefore overly prescriptive requirements would be inappropriate.

14. **Retention limitation: While personal data should not be retained for longer than necessary, some flexibility should be built into the timelines in section 27 for deletion of data and to include further exceptions to address situations where personal data must be retained for legal and/or audit purposes.**

The Draft Act requires that data not be retained for longer than the period prescribed in the Rules for that purpose. Data should be able to be retained as long as necessary for the purposes notified to the data subject, rather than in accordance with arbitrary periods prescribed under Rules. Prescribing fixed retention periods based on the type of purpose is not aligned with International Benchmarks and may stifle innovation as there may be newer purposes that companies wish to use data to innovate with which are not covered by the Rules. This may disincentivise data innovation due to the risk of non-compliance.

The Draft Act should provide enough flexibility to this retention limitation requirement so that deletion of data is not required where it is not technically feasible to comply, where deletion or destruction would prevent organisations from performing a contract or providing a service requested by a user, and where the data must be retained for disaster recovery or legal/compliance purposes. Flexibility for retention is needed particularly where an organisation holds automated backups of data that are scheduled to be deleted, destroyed or de-identified - these deletions are already scheduled and should be enough to demonstrate compliance with this retention limitation requirement.

Inspiration can also be taken from Singapore's PDPA which permits organisations to retain personal data where it is necessary for any legal or business purposes. This ensures that organisations are able to retain data where necessary for future disputes or compliance purposes.

15. **<u>Data-audits</u>: The requirements to perform independent data protection audits whenever required by the Regulator, to allow the regulator to appoint an external auditor, and to call for information, under sections 29, 36, and 40 are of serious concern and should be deleted.**

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.

The investigative powers in section 29 and section 36 are extremely broad and far-reaching, in particular the power to obtain access to all data and to all information necessary for the performance of its tasks, including to obtain access to any premises, equipment and means is particularly invasive, while the proportionality and necessity of on-site inspections in this context are not obvious. It is unclear if the Data Protection Office's decision to conduct an on-site inspection and/or request information must be communicated to the company concerned in advance and with which notice period. In addition, the corrective powers to order the suspension of data flows to a recipient country or international organisation should be removed as this may undermine data privacy and security, harm local businesses and the Bangladesh economy, and break the network connections that are necessary for the internet to function.

The procedure for the request of information or decision to require information should be laid out in the Draft Act and should specify that the request for information should always be proportionate, appropriately motivated, clear and specific. Any time-limit established by the Data Protection Office to provide information should be reasonable and open to extension requests for companies, should it be necessary to comply with the request. Appropriate additional guarantees should be included in case confidential business information is concerned and that such requests would be in full compliance with the Act itself regarding the protection of personal data and privacy. Moreover, insofar as this audit concerns user data, this could potentially create conflicts of law. Companies that are based in the United States are subject to U.S. law, which places strict limits on their ability to disclose contents and most metadata. For government access to user data, we urge Bangladesh to consider diplomatic channels, such as signing a Mutual Legal Assistance Treaty (MLAT) with the United States, and acceding to the Budapest Convention. These steps would create reliable legal channels through which law enforcement officials in Bangladesh could request digital evidence and avoid potential conflicts of law.

The requirement for to submit to regular or ad hoc data audits will be extremely costly and onerous for all data controllers. Data audits are typically extensive exercises and mandating that all organisations (irrespective of their place or line of business) appoint an external auditor authorised by the Director General would increase their annual costs. This would be particularly unsustainable for small businesses, for example a small retail store, who may not have the means to conduct such an audit on an annual basis. It would also create compliance complications for foreign data controllers, especially given that the audit would have to be conducted by an auditor authorised under the Draft Act.

Furthermore, this audit requirement may also cause companies to reconsider opening or doing business in Bangladesh since this poses a risk to their confidentiality obligations and sensitive business information.

16. **<u>Record-keeping</u>: The obligation to keep records in section 27 should be limited only to keeping data subject requests received by the data controller. These records should also only be kept for a limited time.**

The obligation to keep "all" records "regarding the data processed" is contrary to the obligation on controllers under section 25 to "permanently delete" data when no longer necessary for the purposes for which it was collected. It is also contrary to the principle of data minimisation as contemplated by the Draft Act and established international privacy norms. Furthermore, section 27 will result in data controllers retaining data and sensitive personal data for longer, will disincentive the use of privacy protective practices such as pseudonymisation and anonymisation and will increase the risks to individuals should that data be breached. There is also no limit on the time such records must be kept for. We understand that other record-keeping obligations, such as those under anti-money laundering laws of Bangladesh do not ordinarily obligate reporting organizations to retain information longer than five years. An unlimited and expansive record-keeping requirement is unduly onerous and may result in exorbitant costs for companies to keep overly broad records for an unlimited period. This would be especially difficult for smaller local companies to comply with and discourage the collection and use of personal data, which would ultimately have the effect of stifling innovation in Bangladesh.

17. **<u>DPO</u>: Minimum thresholds should be met before a data controller is required to appoint a data protection officer ("DPO") in section 31. The Draft Act should avoid prescriptive requirements on the qualifications of the DPO and should clarify that the DPO function can be outsourced. The Draft Act should also expressly clarify that the DPO will not face personal liability under the Draft Act.**

DPOs play an important role in ensuring an organization complies with privacy laws and facilitating the exercise of data subject rights.

In light of the expansive extraterritorial scope in the Draft Act, the DPO requirement is extremely broad and effectively requires every single organization globally to appoint a DPO. We therefore suggest that minimum thresholds be introduced before the DPO must be appointed, similar to that under Article 37 GDPR. For example, only organizations whose core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or that consist of processing on a large scale of sensitive personal information should be required to appoint a DPO. This approach would also help smaller local businesses who may have limited staff and resources from having to appoint a DPO, which may not be possible given their small staff and budget.

In addition, we recommend that the Draft Act and further Rules avoid imposing prescriptive requirements regrading the qualifications of a DPO. Overly detailed qualification requirements would be onerous for small and medium businesses who may not be able to engage such individuals. We recommend that the focus in this regard be placed on the outcomes of the person engaged as a DPO rather than on their individual qualifications.

We recommend that the Draft Act should clarify that the DPO function can be outsourced. This would be aligned with the best practice position under the Singapore PDPA and will allow

international organisations greater flexibility with appointing a common group-level DPO for better management and oversight. This approach also benefits smaller businesses who may not have internal resources to have a dedicated DPO function, but who would be able to work with trusted external providers to ensure that data subject requests and other privacy queries are attended to.

We understand that the functions and duties of the DPO in section 31(2) will be prescribed under further Rules. We recommend that instead of instituting prescriptive duties for a DPO which may not be suitable for all types of organisations of varying sizes and industries, that the role of the DPO be simply to facilitate the organisation's compliance with the Draft Act. This would allow sufficient flexibility for organisations to structure the position, whilst still ensuring that the core aims of a DPO are met.

Finally, the Draft Act should expressly clarify that the DPO will not face personal liability under the Draft Act. This is vital to ensure the attractiveness of Bangladesh to international businesses. The risk of personal liability for such appointees will deter individuals from taking up the role, and also discourage international businesses from setting up a presence in and investing in Bangladesh as the risks to their employees may outweigh the benefits. Personal liability for the DPO would run counter to the established principle of company law that the organization is a separate legal entity and is therefore out of step with several International Benchmarks.

18. **<u>Data subject rights</u>: The data subject rights in Chapter VI should have clearly articulated reasonable limitations, in line with International Benchmarks, and should also avoid having overly prescriptive mandatory processes under the Rules to be issued.**

Fundamental privacy principles, as enumerated in international privacy frameworks such as the APEC Privacy Principles, state that individuals should have certain rights with respect to their personal data.

Recognising the reasonable limits of practicality and feasibility, these fundamental privacy principles laid out in international privacy laws strike a balance between the rights given to individuals and the compliance obligations placed on organisations. This balance recognises that such rights are not absolute and must be proportionate taking into consideration the function of society and the economy.

With this in mind, best practice internationally includes clear and reasonable limitations on these rights. For example, if allowing access to the data would reveal confidential commercial information or information that could reasonably interfere with the rights of others, the organization should be allowed to refuse the request. Limitations on rights are also provided where the requests are repetitious, systematic, frivolous or vexatious in nature.

International standards also acknowledge that while organizations should respond to such requests as soon as reasonably practicable, privacy laws should not prescribe arbitrary timeframes for responding as each individual request is unique and of varying complexity.

The Draft Act provides very limited exceptions to these data subject rights and states that these will be prescribed in Rules. In practice, there are many situations and circumstances where it is reasonable for organizations to refuse some or all of a data subject request which we recommend are included in the text of the Draft Act. For example, a data controller should be entitled to refuse an access request where such access is likely to adversely affect another's rights, or would

compromise the intellectual property considerations of the Controller. Furthermore, a data controller should only be required to cease processing if a data subject has withdrawn their consent if such processing was originally based on the data subject's consent.

The Draft Act should include reasonable limitations on data subject rights, which align with international best practice, such as the GDPR and Singapore's PDPA. The reasonable limitations to data subject rights should be extended to all data subject rights (not just the right of access and correction), and should be expanded to include situations where complying with the request would:

- disclose trade secrets or proprietary information;
- compromise the privacy or security of the personal data of another individual;
- be infeasible on technical grounds or require disproportionate effort;
- require re-identifying or otherwise linking information that is not considered personal data;
- interfere with law enforcement, judicial proceedings, and/or investigations;
- undermine efforts to guard against, detect, or investigate malicious, unlawful, or fraudulent activity or enforce contracts;
- violate laws or the rights of others;
- involve non-human understandable data;
- facilitate substantially similar, repetitive and/or vexatious requests.

In relation to the right to correct under section 14 (read together with section 20), we understand that the process for submitting data correction requests by data subjects, the manner in which these requests must be fulfilled by the data controllers, and other related matters will be prescribed by rules, which could result in an overly prescriptive regime. We suggest that the rules should ensure flexibility around these requirements since the data controller should be permitted to determine how best to receive and respond to these requests as appropriate for their business processes. Overly prescriptive processes could result in significant costs for small businesses and other organisations who may have to overhaul the way they do business altogether to comply.

The right to erasure (right to be forgotten) under section 18 should also be amended to clarify that the data subject shall have the right to obtain from the data controller the erasure of personal data which they have provided to the controller.

The "right to prevent processing" in section 19 should be deleted. As currently drafted, the right to prevent processing is broad and open to interpretation. There is no clarity as to what "unwarranted substantial damage" entails. The fact that this damage or distress may be to a person other than the data subject also broadens this right substantially and makes it difficult for organisations to understand when this right would apply. In situations where this is likely to be damage or distress caused, it is likely that other bases, such as right of erasure and/or withdrawing consent, would already be sufficient to address this, so this additional right is not necessary.

19. **<u>Accountability:</u> There should be clear avenues in which a data controller can be "deemed" under section 21 to have demonstrated that it has implemented sufficient controls to ensure processing undertaken on its behalf is compliant with the Draft Act, instead of the overly broad requirement to demonstrate that all such processing is compliant.**

Whilst we agree that data controllers should be ultimately responsible for all data processed by both themselves and their appointed data processors, it is unreasonable to expect the data controller to at any time demonstrate that their data processor is compliant with the Draft Act as this would be almost impossible to do.

Outsourcing and engaging data processors is a vital part of cost and strategic management, and is an unavoidable part of almost all businesses these days. Data processors range from cloud services providers, logistics delivery partners, accounting firms and security companies. Requiring data controllers to be able to demonstrate compliance by all its vendors is an unreasonable and almost impossible task as data controllers cannot reasonably be expected account for every single act of the data processor. We therefore recommend that data controllers instead be required to implement reasonable oversight measures and controls through binding contractual obligations, and that where they have reasonably fulfilled their oversight responsibilities in this regard, they not be held liable for any acts or omissions by a data processor not within their control.

20. **Penalties and sanctions: There are administrative fines prescribed for various types of breaches of the Draft Act, but the Director General also has discretion under to deem any breach of the Draft Act (where brought as a complaint) an offence and subsequently the court may impose criminal fines and/or imprisonment as well.**

These provisions therefore have the potential to impose both administrative fines and criminal fines (and imprisonment) for the same breaches. This creates uncertainty as to the penalties that apply in specific situations. In particular, we recommend deleting section 58 so that only administrative fines apply as a default, with no general criminal liability. The inclusion of criminal offences creates an adversarial environment that discourages collaboration between regulators and data controllers.

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.

Criminal penalties should be reserved for more egregious breaches of the Draft Act . For example, section 51 of the April 2022 version of the draft Act imposed criminal penalties for knowing, intentional or reckless collection or disclosure of sensitive data that results in loss to the data subject. We note that the current Draft Act has instead expanded section 51 to apply to

all data rather than only “sensitive data” which is a less reasonable approach. Adopting a measured approach where criminal penalties are only imposed for serious breaches would strengthen the trust and co-operation between organisations and regulators to ensure that compliance and enforcement are seen as fair and commensurate.

In relation to the criminal fine that may be imposed by the court under section 58, we note that there is no direction or guidance on how the judiciary should exercise its discretion, or general sentencing guidelines, or mandate to take graded approach, the courts can impose maximum penalty of BDT 1,000,000 and/or imprisonment of up to 3 years in any case. Therefore, we also suggest incorporating principles of due process and proportionality guardrails to avoid judicial overreach.

In addition, we suggest removing the position in section 55(2) that unpaid administrative fines are recoverable as a public demand under the Public Demand Recovery Act, 1913. When a debt is recoverable as public demand, the government can recover it: (i) by attachment and sale, or by sale (without attachment), of any property; (ii) by attachment of any decree; or (iii) by arresting the debtor and detaining him. This is disproportional to the nature of the breaches in this case and therefore out of step with International Benchmarks.

21. **Penalties and sanctions: The personal liability of directors for offences committed by a company under section 62 should be deleted in its entirety.**

Personal liability should only be imposed on individuals who have actually committed an offence under the Draft Act, with criminal liability only imposed for deliberate, repeated or egregious breaches, as mentioned above. “Deeming” such individuals guilty also goes against the general principle of the presumption of innocence that underpin criminal law regimes.

Furthermore, since the Draft Act seeks to regulate offshore entities as well, this personal liability provision would have even more far-reaching implications for international businesses whose executives would then be joined in any relevant trials in Bangladesh, which would certain have a negative impact on international companies’ willingness to do to business in Bangladesh.

22. **Penalties and sanctions: Section 54, which imposes an arbitrarily higher financial penalty on foreign companies who breach the Draft Act, should be deleted.**

There is no reason why a company, by virtue solely of it being a “foreign company” registered under the Company Act, should be subject to a potentially much higher fine for exactly the same breach that may have been committed by a local company. This is inconsistent with International Benchmarks and principles of fairness under the law.

There may also be an unintended effect of discouraging international companies to offer their products and services to the Bangladesh market, which would be detrimental to consumers. It may also render the foreign company registration regime pointless and unutilised since no company would want to be registered as such if the consequence is arbitrarily higher fine limits.

23. **Personal data protection principles: Section 5 should be deleted in its entirety and moved to a code of conduct or practice direction issued under section 38 of the Draft Act.**

This section introduces unnecessary confusion and overlap into the Draft Act. The drafting of the explanatory text to each principle is extremely unclear and creates confusion. The general

principles are already addressed in more detail in the sections in Chapter III of the Draft Act, so removing this overlap would help to eliminate confusion. If necessary, we suggest that these general principles are more appropriate to be framed as code of conduct or practice direction under Section 38 of the Draft Act.

24. <u>Anonymised data</u>: The definition of "anonymised data" in section 2(a) should be revised to a more general and technology-neutral definition, which does not reference prescribed processes under the Draft Act.

Standards of anonymisation should consider whether there is a serious possibility that an individual could be re-identified having regard to all the means which are likely to be reasonably used for that purpose. This approach would be aligned with comparable provisions in laws of other countries, such as Singapore and EU.

The GDPR also excludes anonymised data, defined as data which can no longer identify a natural person. It specifies that to ascertain whether a natural person is identifiable, "account should be taken of all the means reasonably likely to be used" for re-identification, including objective factors such as time required for the effort, available technology.

We suggest that the definition be amended to read "anonymised data means data which cannot, directly or indirectly, reasonably identify an individual whether from that data alone or with other information in the possession of a data controller". The current definition implies that there is a prescribed process of anonymisation under the Draft Act that must be adhered to. As appropriate anonymisation techniques may vary based on the circumstances and technological developments, laws should generally be future-proof and technology-neutral and allow a degree of flexibility in appropriately achieving anonymisation. This is especially important since organisations have greater flexibility in using anonymised data, and anonymised data sets are consequently often used for innovation and business improvements. A lack of clarity here or an overly prescriptive definition of anonymised data would hinder such innovation and development.

25. Profiling: The definition of "profiling" in section 2(k) should be clarified and aligned with International Benchmarks such as those in Article 4(4) GDPR.

The newly included of definition of "profiling" is extremely broad as it is defined as "any act of collecting useful information or data of a person where description of necessary information or data of such person is inserted/compacted". This is unclear and could ultimately include almost all types of processing of data that is then combined with other derived data or original inputs from the data controller.

It is important to have a clearly defined scope of "profiling" since this impacts the jurisdictional scope of application of the Draft Act in section 4. As the Draft Act applies to overseas entities that undertake "profiling" activities, it is important to ensure this is clearly and appropriately scoped so that it is clear who the Draft Act applies to.

We recommend that the definition of "profiling" be aligned with Article 4(4) GDPR which defines it as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

26. **<u>Data breach notification</u>: The timelines to be prescribed under section 28 for notifying the Director General of data breaches should not be unduly prescriptive.**

There is a new requirement for data breaches to be notified to the Director General "without undue delay and where reasonably possible, not beyond the period as may be prescribed." We recommend that any prescribed timelines be flexible enough so as to allow organisations who have suffered a data breach to properly investigate the breach and understand the extent and severity of it before having to notify the Director General.

All data breaches are different and in some cases, more complex breaches require thorough assessment. If there are strict timelines that must be complied with, this may sometimes result in organisations taking a notify-first-investigate-later approach which may result in the Director General being inundated with breach notifications for suspected incidents which are not actual data breaches or for low risk events. This would place an undue administrative burden on the Director General and may inadvertently divert resources away from investigation and attending to actual high-risk data breaches. We recommend that the wording in the April 2022 version of the draft Act, which only required notices to be made "without undue delay", be reinstated as this provides sufficient flexibility and accountability in data breach reporting. It should also be made clearer that any timelines for reporting start only once an organisations has *assessed* that a data breach has taken place. This position would be aligned with International Benchmarks such as Singapore's PDPA.

27. **<u>Personal data of children</u>: Prescriptive age verification and parental consent processes should be avoided in section 12(3) in relation to personal data of children, and more flexibility should be given to organisations to determine what is most appropriate and reasonable to implement in the circumstances.**

The age of consent to access online services should be distinguished from the age of majority in other contexts. The level of maturity and cognitive development required, for example, to serve in the military, drink alcohol, vote, or be held criminally liable involved consideration of a variety of factors that are meaningfully different from what should be required to visit a website, download an app or participate in online educational activities.

This evaluation must be grounded in a data-driven evaluation of the harms we are seeking to prevent, the impact to teen's rights of participation and autonomy, and what we know about teen's evolving capacity to understand and avoid potential risks involved. This is supported by the 2018 UNICEF guidance on Children's Online Privacy and Freedom of Expression, which includes a key principle that "Children's privacy and freedom of expression should be protected and respected in accordance with their evolving capacities."

Research shows that teens tend to be quite knowledgeable when it comes to understanding data collection practices and controlling the information they share online. In fact, a McAfee Study "Teens, Tweens and Technology" found that teens today -- so-called "Digital Natives" -- are often more tuned in to tech-issues than parents — and while parents are also familiarizing themselves swiftly with the tech their children use, there is still a gap to be bridged. It is important to note that GDPR only requires parental consent for minors under the relevant AoC when the legal basis for data processing is consent. Parental consent requirements under GDPR are not a complete bar to accessing the service.

In the US (COPPA), children under 13 years are not barred from accessing digital services, however, prior verifiable parental consent is required for services that are directed at users under 13 or if there is actual knowledge that there are users below 13 years of age on the service.

In evaluating the best interests of the child, we are guided by the UN Convention on the Rights of the Child which directs us to consider the child's safety, psychological and emotional development, identity, freedom of expression, privacy and agency to form their own views and have them heard.

Children have a right to be heard and should benefit from online communities. Online education and skill development have taken on even more importance through the COVID-19 pandemic, with the internet being the only avenue that children have to continue learning. We recognize how crucial it is to extend educational resources to young Bengalis. Access to these tools also enables them to build digital skills, awareness of online risks, and resilience in a more protected environment as they continue their journey toward adulthood.

Rather than restricting the internet usage of any individual, privacy legislation should focus on creating a regulatory environment whereby controllers are required to surface only age appropriate content, develop privacy and safety protections, and educate teens, parents and guardians about their rights and responsibilities online.

It's important to 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. Parents are not in the position to actively oversee every interaction their teen has online, nor should they be expected to. Instead, companies should be encouraged to build protections into their services that shield younger users from potentially risky interactions or content .

Additionally, a stronger approach than the Draft Act's approach to age verification might be for industry to work with the regulator in preparing Codes of Practice around verification processes. As industry standards evolve and become more robust, so can the Codes. 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.

We understand that further rules will be prescribed on the processes that must be implemented for age verification and parental consent when personal data of children is collected and processed. Imposing prescriptive age verification and parental consent mechanisms or processes could be unduly prohibitive and may not be appropriate to the specific circumstances of personal data collection or processing. For example, if certain technological measures must be implemented, these may be onerous for smaller businesses whose customer base may include children (e.g. local toy stores or educational websites) and may stifle innovation by smaller, local companies in Bangladesh.

28. <u>PDPO</u>: While we support the establishment of the Data Protection Office under sections 35 to 37, the head of the Data Protection Office should be separate and independent from the head of the Digital Security Agency.

Privacy laws and frameworks benefit from being applied consistently across different industries. This assures individuals that they can expect a baseline level of privacy protection in all situations where their personal data is being processed.

To facilitate such a consistent, cross-industry approach, it is best practice to consolidate oversight of privacy matters in one central, independent regulator. This privacy regulator is generally a newly established regulator with a broad understanding of multiple industry sectors.

In data-driven economies, privacy and digital innovation are often considered hand in hand as they are closely interlinked. This approach can help to align the independent regulator's activities with broader goals of promoting and supporting its digital economy.

Personal data protection encompasses more than just digital security, as any legislation must also balance digital innovation and the individual's right to privacy. It would be preferable to appoint a separate, independent person to oversee the Data Protection Office who would be better placed to mediate between these priorities instead of only focusing on data security. An over-emphasis on data security may, in some cases, result in overly conservative policies that may stifle innovation and development rather than ensure that it takes place in a responsible way.

29. **Investigations: While we support the powers of the Director General and Data Protection Office to carry out investigations under the Draft Act, we recommend that timelines for these investigations be introduced to align with other Bangladeshi laws.**

Under DSA, for example, an investigation is required to be completed within 60 days from the date of its commencement, and any extension not exceeding 15 days must be approved by a superior officer. For any further extension, the investigating officer must give the cyber tribunal a written report stating the reason for additional extension, and thereafter, with the permission of the tribunal, complete the investigation in the next 30 days. We also understand that the High Court Division of the Supreme Court of Bangladesh has recently directed law enforcement agencies to comply with this timeline, as investigations under DSA are not being completed on time. Aligning the timelines as such enhances certainty for companies under investigation and minimises the potential for unduly long investigations.

30. **Interaction with other laws: We support the clarification in section 3 that the Draft Act takes precedence over any inconsistent provisions in other written law but suggest that further clarifications on the Draft Act's relationship with the DSA be included.**

The DSA also contains language in section 3 that it should prevail over any other law in the event of an inconsistency. However, the Draft Act and the DSA have some overlaps, for example in relation to the unauthorised use of data (see sections 26 and 33 DSA). A data controller could therefore be liable under both the Draft Act and DSA. It would therefore be helpful to expressly repeal Sections 26 and 33 of the DSA for consistency with the Draft Act. We understand that the DSA has in the past repealed several provisions in the Information and Communication Technology Act, 2006 to avoid the overlap, so this is possible. Alternately, the Draft Act should be expressly given precedence over DSA in express terms, to the extent there is inconsistency.

31. **Consent withdrawal and services:** We recommend amending section 15 to clarify that controllers will not be mandated to provide products and services that require personal data after the withdrawal of consent.

The Draft Act provides users with the right to withdraw consent to the processing of data under section 15, but does not specify whether businesses are still expected to provide goods and services after the right is exercised. While we are supportive of the inclusion of data subject rights

within the Draft Act, businesses frequently rely on user data to provide products and services. Without processing user data, it may not be technically or economically feasible to provide products and services that a user has requested

To address this potential conflict, the Draft Act should be explicitly amended to make it clear that controllers are not required to provide products or services that require the personal data of an individual user if the user has exercised their right to withdraw consent. By adopting this clarifying language, the Draft Act will retain protections for user data and become more feasible for businesses to implement.

B. CONCLUSION AND NEXT STEPS

We reiterate our support for Bangladesh's efforts to introduce personal data protection legislation, and we respectfully encourage [Ministry of Posts, Telecommunications and Information Technology] to engage in further dialogue with industry to consider the broader issues and implications before the Draft Act is finalised.

We believe these recommendations will help ensure the creation of a privacy regime that ensures Bangladesh benefits from the economic gains created by uses of data by creating strong protections for Bangladeshi citizens while enabling cross-border data flows and flexible approaches to the use of data.

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. Importantly, 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 around effective data protection framework in Bangladesh.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)