29 May, 2023

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 (AIC) On The Draft Data Protection Act, 2023

Dear State Minister Palak,

On behalf of the Asia Internet Coalition ("**AIC**") and its members, I am writing to express our sincere gratitude to the Information and Communication Technology Division for leading the drafting process of the new Data Protection Act 2023 and for the opportunity to submit comments on the latest draft published on March 14, 2023 (the "**March 2023 Draft**" or "**Draft Act**").

AIC is an industry association of leading internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of internet and information and communication technology policy issues, and are fully committed to the cause of a safe and open internet.

We commend the continued engagement by the Government of Bangladesh with the civil society and industry partners in drafting this important legislation to align with global best practices. While we were pleased to see some positive changes in the March 2023 Draft, such as a three year implementation window, providing two new principles of data protection, and allowing for cross-border enforcement cooperation, a number of significant concerns remain unaddressed. These provisions can benefit from further review and revision, to account for diverse social, economic, and innovation-oriented objectives, and to avoid roadblocks to innovation and technological advancement in Bangladesh.

We firmly believe that a privacy-centric and business-friendly framework will not only allow local businesses to participate and flourish in the global stage and attract international investment in the country's digital ecosystem, it will also allow Bangladesh to achieve its digital

economy goals whilst still protecting individual privacy and instilling citizens' confidence in the data protection regime. With Bangladesh now integrated with the global technology ecosystem and home to a growing data-driven digital economy, the introduction of a balanced data protection law is timely and imperative.

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

A. COMMENTS AND RECOMMENDATIONS

1. Scope of application: The Draft Act should clarify that it applies only to those data that directly or indirectly identifies an individual, and all reference to "data" should be deleted entirely.

As currently drafted, the Draft Act applies to any and all forms of data, which is defined as "formally prepared information, knowledge, event, concept or instruction, which has been processed, is being processed, or will be processed in a computer system or computer network in any form or format, including computer printout, magnetic or optical storage media, punch card, punch tape, or which is retained in any computer memory, and for such purposes shall include personal data … [but] shall not include any anonymized, encrypted or pseudonymized data that cannot identify a single individual." However, the March 2023 Draft does not define the term "personal data."

Effective data protection and privacy laws around the world extend their scope to information that relates to natural persons who are identified or identifiable, and not to data in its abstract sense. This is because mishandling personal data could have a big impact on an individual's life. 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, and therefore does not require equal level of protection as personal data. Imposing additional protections on non-personal 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.

We recommend that the Draft Act make clear that it only applies to personal data, i.e., data that can identify an individual, and all reference to "data" should be deleted entirely.

2. Data storage in Bangladesh: Mandatory data localization in respect of sensitive data, user-generated data, and classified data should be deleted in its entirety.

We note that the data localization requirement has been revised in the March 2023 Draft: while previously sensitive data, user-generated data, and classified data were required to be stored

only in Bangladesh, the current draft allows companies to store data outside the country as long as they also maintain data residency in Bangladesh.

Decisions about where to store data should be based on technical considerations of the global internet, organizational capacity, and users' needs, instead of being driven by data sovereignty. This is the best way to ensure providers can deliver strong performance, reliability, and security to their users. Storing these 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.

Requiring default data localization for sensitive data, user-generated data, and classified data would cut Bangladesh off 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 serve global customer bases host their websites, apps, products, and services, and process user data across data centers located around the world. In other words, user data is distributed across various servers globally — irrespective of the geographic origin of any data. These global data centers are the foundation of the global infrastructure of the internet, and being able to transfer data internationally, and store it in these data centers, 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 decentralizing data storage and making state-of-the-art cyber defenses accessible and affordable to companies irrespective of their size, thus making personal and sensitive data less vulnerable to malicious actors. Malicious third parties can often target jurisdictions whose cybersecurity defenses are not up-to-date because they are cut off from state-of-the-art services, exacerbating security concerns instead of resolving them.

Furthermore, it is unclear why there is a distinction made specifically for user-generated data to be stored in Bangladesh by default under section 44 – 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 "any private data of a data subject (for example text, message, images, videos, audios, reviews, email or any other private documents or similar other subject matter) which are created or generated by an individual or a group of individuals for limited use or share and not intended for public use." No data privacy and protection legislation around the world requires mandatory special protection for such vague classes of data. Regulating user-generated data is more appropriate for online content regulations, and not data protection legislations.

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 Draft Act 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 localization 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 centers located in Bangladesh. From a technical standpoint, this localization requirement could be seen as requiring 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. Data localization requirements will be extremely expensive and operationally and technologically difficult, if not impossible, to implement for companies of all sizes – in particular small and medium-sized enterprises lacking the resources or infrastructure to accomplish this. It will also artificially limit the ability of such enterprises by making it harder for Bangladeshi businesses to harness the value of the data, stifling innovation and economic growth, and reducing productivity. Furthermore, 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. In the long term, the data localization mandate will invariably hamper the Bangladeshi economy.

As such, we recommend deleting this section from the Draft Act in its entirety.

3. **Cross-border transfers: Cross-border data flows in respect of sensitive data, user generated data, and classified data should be amended to allow transfers in a broader range of circumstances.**

Cross-border data transfers are integral to the functioning of the internet. 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 decentralized 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 optimize routing in real time to reduce latency and increase network resilience.

Cross-border transfer of sensitive data, user generated data, and classified data is allowed subject to obtaining user consent, or meeting certain conditions (e.g., for inter-state commerce, international relations, or any other matter specified by the government). While we welcome the revision made to the March 2023 Draft removing the requirement to notify the Director General for each instance of data transfer, we have significant remaining concerns that the

provisions of section 45 are too restrictive and vague on the requirements around cross-border data transfers. Imposing prerequisites on cross-border transfers of sensitive data, user generated data, and classified data, like obtaining user consent or meeting certain conditions (e.g., for inter-state commerce, international relations, or any other matter specified by the government), would make it extremely challenging to run a business out of Bangladesh or serve Bangladeshi consumers since there would be so much uncertainty around whether the provider could transfer data.

Furthermore, it allows other regulators – such as the Bangladesh Bank, the Bangladesh Telecommunication Regulatory Commission, and the National Board of Revenue – to make sectoral regulations to regulate cross-border transfer of data that falls within their jurisdictional mandate. This could create a patchwork of regulations governing cross-border data flows, as a result of which companies may have to comply with different requirements with respect to data transfer outside Bangladesh set by each regulator. For example, tax and financial data sent via user-generated content hosts could potentially be regulated by the central bank, the tax authority, and the data protection agency, resulting in confusion and uncertainties for businesses.

While we agree with the underlying intent to deliver secure services for the citizens of Bangladesh, legal frameworks that inhibit or restrict cross-border data transfers will make Bangladeshi users' data less secure. Thus, insofar as laws aim to regulate cross-border data transfers, they should be narrowly tailored and built on common principles that give people rights and control over their information, ensuring companies implement robust privacy practices and policies, and holding them accountable when they do not. It is essential that these frameworks facilitate the free flow of data across borders unambiguously and unconditionally.

We recommend extending the legal bases for cross-border transfers to include transfers to approved-listed territories, or where such transfers are necessary for the performance of a contract between the data subject and the data controller, or where such transfers are allowed under approved contractual clauses, an international treaty, a trade agreement to which Bangladesh is a party, or under intra-group schemes approved by the government, or where such transfers are necessary for the provision of services.

Furthermore, we recommend deleting section 45(2) that allows formulation of different sectoral regulations, and encourage the government to frame a single framework on cross-border data transfer.

4. **Personal liability: Provisions allowing personal liability of individuals associated with non-compliant data controllers for offenses committed by the employing company should be deleted in its entirety.**

As currently drafted, section 65 allows lawsuits to be initiated against both a non-compliant company as well as individuals associated with the company, such as the shareholders, directors, chief executive officers, managers, secretaries, partners, and other officers, employees and representatives who were involved with the non-compliance, unless they are able to prove that the non-compliance was committed without each of their knowledge, or they tried their best to prevent the non-compliance. As a general principle, personal liability should only be imposed on individuals who have actually committed an offense under the Draft Act, with criminal liability only imposed for deliberate, repeated or egregious breaches. "Deeming" such individuals guilty also goes against the general principles of the presumption of innocence and the burden of proof that underpin criminal law regimes.

Furthermore, since the Draft Act seeks to regulate non-resident 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 certainly have a negative impact on international companies' willingness to do business in Bangladesh.

We recommend deleting sections 65 so that no personal liability is attached to individuals associated with a company.

5. **Extra-territorial application: The broad extraterritorial application of the Draft Act in sections 4(b) and (c) should be amended.**

As currently drafted, the Draft Act appears to apply to those (a) within Bangladesh who collect and process data, (b) outside Bangladesh who collect and process data of any Bangladeshi citizen anywhere in the world, and (c) outside Bangladesh who process data in connection with any commercial delivery of goods or services in Bangladesh or the profiling of data subjects anywhere in the world. What this means in effect is that the Draft Act will apply to data controllers and processors irrespective of the purpose of data processing activities (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 Bangladeshi citizen as a customer) or to any Bangladeshi customer (since it would apply to the profiling of data subjects anywhere in the world). In order to comply with such a requirement, all companies around the world may have to maintain a database of their customers and information relating to their citizenship, and identify those who are Bangladeshi citizens in order to comply with the legal requirement. This unduly broad and unlimited extra-territorial application may have the unintended effect of causing non-resident 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 the Draft Act to apply extraterritorially. For instance, where an offshore company unambiguously targets the Bangladeshi market, or processes information related to Bangladeshi citizens, it may be relevant for such companies to be subject to the provisions of the Draft Act. We recommend that situations where the law will apply is clearly articulated in section 4 of the Draft Act. Inspiration can be taken from Recital 23 of the GDPR, which states that in order to assess whether a business is offering or envisages offering goods and services to data subjects within a country, factors such as the use of a language or a currency generally used in that jurisdiction, or reference to customers or users who are within that jurisdiction, can be taken into account.

We therefore recommend amending the extra-territorial provisions in sections 4(b) and (c) to align with the international benchmarks.

6. **Legitimate interest as a legal basis: Provisions should be incorporated in section 7 to allow the processing of data on the grounds that the entity has a legitimate interest in processing such data, or the processing is reasonably necessary for the entity's functions.**

While section 7 outlines the legal bases for processing data under the Draft Act, it does not include the well-established "legitimate interest" basis for data processing featured in comparable data protection regimes. 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 instance, organizations use the legitimate interest basis for processing related to operations to guard against unauthorized access by bad actors, malware prevention, and the prevention and detection of security incidents.

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

7. **Rights of foreign data subjects: Ambiguous rights of foreign data subject should be deleted in its entirety.**

The requirement under section 17 is unusual and not aligned with international benchmarks, as well as approaches to privacy laws elsewhere in the region. It appears to require data controllers in Bangladesh to comply with obligations arising under the laws of other jurisdictions, which creates considerable uncertainty.

We recommend deleting this section from the Draft Act in its entirety. To the extent the objective of the section is to afford protection to non-citizens in Bangladesh under the laws of another country, such protection shall apply by operation of law. In any event, the data of such non-citizens are protected under clauses (a), (b), and (c) section 4(1) of the Draft Act.

8. **Government access and requests for data: Requirement to give government access to user data should be amended to align with international frameworks and to avoid conflicts of law.**

The collective effect of sections 10(2)(d), 38(2)(a)(ii), (iv) and (v), 41(1), 42 and 64(1) is to create a framework that allows unfettered government access to data. For instance, section 10(2)(d) allowing collection of any data from a data subject if it is "necessary for the prevention, detection, investigation of an offense or for the national security" is unclear, broad, may create conflicts of law, and is not aligned with international frameworks, and may therefore cause concern for businesses seeking to provide services or operate in Bangladesh. Importantly, data localization requirements and limitations on cross-border data transfers would not resolve these conflicts, and may even exacerbate them. Similarly, sections 38(2)(a)(ii), (iv) and (v) and 42 allow the data protection regulator to access data for the purpose of examination or necessary for its functions, and the data controllers and processors must provide information requested. Concerningly, this provision is broad, and it is not clear if the obligation extends to only user data or all data held by the data controllers and processors. It is also unclear as to how these provisions will apply if they conflict with foreign laws.

We recommend that Bangladesh consider signing mutual legal assistance treaties under the Mutual Legal Assistance in Criminal Matters Act, 2012, with the United States and other countries where the disclosing companies are situated. In addition, Bangladesh should ratify the Budapest Convention in order to facilitate law enforcement requests for data from non-resident service providers.

9. **Sensitive data: The definition of "sensitive data" should be exhaustive, and "financial or commercial data" should not form part of sensitive data.**

As currently worded, the definition of "sensitive data" includes financial, commercial, medical, health data, genetic, and biometric data, as well as data related to the commission or the allegation of offense, legal proceedings, and judgements, and "any other data as may be prescribed by the rules."

Having an exhaustive definition of "sensitive data" would be aligned with international benchmarks and comparable foreign legislations, which typically do not include any powers for the regulator to further expand the list. Sensitive personal information should encompass data about individuals that reveals attributes that are impossible or difficult to change and increase risks to those individuals of discrimination or harm. 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 from earlier drafts. 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 organizations greater certainty over the types of data that are accorded the additional protections under the Draft Act. It is important that the list of “sensitive data” is not uncertain or 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.

Additionally, we note that the term “commercial data” is now defined in the March 2023 Draft. Regardless, 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 and commercial data are 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.

10. Enrollment requirement: Obligation to enroll by data controller and data processor should be deleted in its entirety.

We note that section 46 continues to mandate enrollment of data controller and data processor. Not only is enrollment requirement vague and not consistent with international benchmarks, it is unclear as to what policy objective it seeks to achieve and how the registration will enhance citizens’ privacy rights. To add to the ambiguities and uncertainties, the terms of the enrolment, its renewal and suspension, and other related matters, are stated to be prescribed by the rules. Instead of conferring benefits to companies and consumers, this requirement will impose unnecessary compliance and cost burdens which will dissuade businesses from using data at all, which would stifle innovation and limit choices for consumers. It could also compel non-resident companies to discontinue some or all of their services to consumers in Bangladesh.

We therefore recommend deleting the requirement of enrollment of data controller and data processor in its entirety and unconditionally.

11. Data protection register: The requirement to register all purposes for which data is collected or processed, and share the data protection register with the Director General, should be deleted in its entirety.

Requirement to maintain a data protection register and disclose sensitive and confidential information, and allow unaffiliated third parties to inspect information recorded in the register under sections 47 and 48 is out-of-step with the international benchmarks and not aligned with proportionate objectives of data privacy, and could therefore have several negative effects.

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 regulator. 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 Data Protection Agency. 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 centralized registry of these purposes would mean significant resources would be devoted just to maintain this record rather than on truly ensuring that the regulator is prioritizing 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 privacy as well as confidentiality of sensitive business information.

Lastly, registration does not necessarily lead to meaningful compliance by organizations because even if offshore organizations do in fact register with local regulators, the practical challenges of enforcement against offshore entities still remains, together with the ongoing risk of organizations 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 organizations through complaints and other consumer-initiated actions.

We therefore recommend deleting the requirement to maintain a data protection register in its entirety and unconditionally.

12. Data audits: Obligation 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, 38, and 39 are of serious concern and should be deleted.

Enforcement frameworks are a necessary part of privacy laws and a carefully calibrated enforcement strategy helps to promote compliance. Specifically, leading international frameworks, such as the data protection legislations in the European Union and Singapore,

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. Mandating an audit requirement moves in the opposite direction and will likely create animosity.

Importantly, data audits are typically extensive exercises and mandating that all organizations (irrespective of their place or line of business) appoint an external auditor authorized 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. It would also create compliance complications for foreign data controllers, especially given that the audit would have to be conducted by an auditor authorized under the Draft Act.

Moreover, insofar as this audit concerns user data, this could potentially create conflicts of law. For instance, 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 the government to consider diplomatic channels, such as signing a mutual legal assistance treaty with the United States, and acceding to the Budapest Convention. 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.

We therefore recommend deleting the requirement to maintain a data protection register in its entirety and unconditionally.

13. Data protection officer: Requirement to appoint a data protection officer should be amended so that it is subject to a minimum threshold, and prescriptive requirements with respect to qualifications should be avoided, and the provision should clarify that the function can be outsourced.

Data protection officers play an important role in ensuring an organization complies with the relevant privacy laws and facilitating the exercise of data subject rights. In light of the expansive extraterritorial scope in the March 2023 Draft, the requirement to appoint such an officer by data controller is extremely broad, in that it effectively requires every single organization in the world to appoint an officer, irrespective of their size or nexus with Bangladesh.

We therefore suggest that minimum thresholds be introduced before a data protection officer is required to be appointed, similar to that under the GDPR, which requires an offer to be appointed by only those 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 consists of processing on a large

scale of sensitive personal information. This approach would also help smaller local businesses who may have limited staff and resources from having to appoint a data protection officer, which may not be possible given their limited resources.

In addition, we also recommend that the Draft Act and further rules avoid imposing prescriptive requirements regarding the qualifications of a data protection officer. 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 data protection officer rather than on their individual qualifications.

We also recommend that the Draft Act should clarify that the functions of the data protection officer can be outsourced. This would be aligned with the best practice position under the Singaporean law and will allow international organizations greater flexibility with appointing a common group-level officer for better management and oversight. This approach also benefits smaller businesses who may not have internal resources to have a dedicated officer, but who would be able to work with trusted external providers to ensure that data subject requests and other privacy queries are attended to.

Finally, the Draft Act should expressly clarify that the data protection officer will not face personal liability for non-compliances of the data controller. 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 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.

14. **Penalties and sanctions: Discretion of the data protection regulator to "deem" a non-compliance as a criminal offense, and subject companies and individuals to criminal fines and imprisonment, are of serious concern and should be deleted in its entirety. Furthermore, the discriminatory penalty regime against a "foreign company" should also be deleted in its entirety.**

While the provisions on administrative fines for various non-compliances are acceptable, sections 60(1) and 61 allows the Director General to discretionarily consider a violation under the Draft Act to be a criminal offense, for which the court can impose a criminal fine and/or imprisonment. 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. The inclusion of criminal offenses creates an adversarial environment that discourages collaboration between regulators and data controllers. 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 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. 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 maximizes voluntary compliance.

We recommend deleting sections 60 and 61 so that only administrative fines apply as a default, with no general criminal liability.

In relation to the criminal fine that may be imposed by the court under section 61, 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, and as such the courts can impose maximum penalty of BDT 1,000,000 and/or imprisonment of up to 3 years in any case. Therefore, we recommend incorporating principles of due process and proportionality guardrails to avoid judicial overreach.

We also recommend removing the position in section 58(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 disproportionate to the nature of the breaches in this case and therefore out of step with international benchmarks.

Finally, we recommend deleting the discriminatory provision that penalizes a “foreign company” registered under the Company Act, 1994. There is no reason why a company, by virtue solely of it being a “foreign company,” 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 un-utilised since no company would want to be registered as such if the consequence is arbitrarily higher fine limits.

B. CONCLUSION AND NEXT STEPS

We reiterate our support to the Government of Bangladesh in its efforts to introduce new data protection and privacy legislation, and respectfully encourage the Information and Communication Technology Division to engage in further dialogue with industry to consider the broader issues and implications before the Draft Act is finalized.

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

We will continue to be a constructive partner for the Government of Bangladesh in considering these important legislative and policy matters, and the best way to approach them, and welcome the opportunity to offer our inputs and insights directly through meetings and participating in the official discussions.

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)