7 July 2020

Mr. Zunaid Ahmed Palak
Hon'ble State Minister
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
Government of the People's Republic of Bangladesh
E-14/X, BCC Bhaban, Agargaon, Dhaka – 1207
Bangladesh

SUB: INDUSTRY SUBMISSION ON THE DRAFT INFORMATION PRIVACY AND SECURITY RULES, 2019 AND THE DIGITAL SECURITY AGENCY RULES, 2020

Dear Hon'ble Minister,

On behalf of the Asia Internet Coalition ("**AIC**") and its members, I am writing to express our sincere gratitude to the Government of People's Republic of Bangladesh ("**GoB**"), and in particular the Information and Communication Technology Division ("**ICT Division**"), for its efforts in undertaking various initiatives to bolster the legal and regulatory regime on digital security and data privacy in Bangladesh and to address the present day concerns and challenges with respect to burgeoning technological developments and the needs of the ICT market in Bangladesh. In particular, we welcome the recent enactment of the Digital Security Agency Rules, 2020 ("**DSA Rules 2020**") and the initiative taken to draft the Information Privacy and Security Rules, 2019 ("**Privacy Rules**"), to further upgrade the regulatory framework in Bangladesh.

The AIC is an industry association comprised of leading internet and technology companies, and is committed to promote the understanding and resolution of the internet and ICT policy issues in the Asia Pacific region. Our current members include Facebook, Google, Amazon, Apple, SAP, Cloudflare, Airbnb, Booking.com, Expedia Group, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media).

We commend GoB's commitment to the objectives of Digital Bangladesh, including safeguarding the fundamental rights under Article 43 of the Constitution of Bangladesh, and implementing its obligations under various international treaties and conventions, including the International Covenant on Civil and Political Rights. These efforts in strengthening the legal and regulatory framework are timely and necessary, driven largely by the visionary policies and initiatives adopted and implemented by the GoB, at a time when Internet penetration in Bangladesh has reached 41% in January 2020 (the number of internet users in Bangladesh increased by 5.8 million (+9.5%) between 2019 and 2020, exceeding 100 million for the first time to reach 103.253 million users. In response to these policies and unprecedented increase in the internet penetration, Bangladesh IT and IT-enabled service (ITES) sector will be the main partner of the government in materialising the vision of Digital Bangladesh. In Bangladesh, more than 120 companies export information and communications technology (ICT) products worth nearly US$1 billion to 35 countries. By 2021, it's expected that this will increase to US$5 billion. Indeed, the growing strength of the ICT Industry underpins the vital pillars that will support Bangladesh's transformation to a digital economy by 2021, and a knowledge economy by 2041.

While we support these efforts, there are some ***serious*** concerns about the DSA Rules 2020 and the draft Privacy Rules that we would like to express. As such, please find appended to this letter detailed comments and recommendations with respect to the DSA Rules 2020 and the draft Privacy Rules, which we would like to respectfully request the ICT Division to consider.

We appreciate the opportunity to participate in discussions with the GoB and provide input into the policy-making process. We would be happy to offer our inputs and insights directly through meetings and participating in the official consultations.

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. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)
www.aicasia.org

Cc:

1. *Mr. Mustafa Jabbar, Hon'ble Minister, Ministry of Posts, Telecommunications and Information Technology*
2. *Mr. Sajeeb Wazed Joy, Information and Communication Technology Advisor to the Government of Bangladesh*

Enclosed:

1. Enclosure A: Detailed comments and recommendations on the draft of the Information Privacy and Security Rules, 2019
2. Enclosure B: Detailed comments and recommendations on the Digital Security Agency Rules, 2020

Enclosure A

DETAILED COMMENTS AND RECOMMENDATIONS ON THE DRAFT INFORMATION PRIVACY AND SECURITY RULES, 2019

A. General Comments

The Constitution of Bangladesh ("**Constitution**"), adopted on 4 November 1972, guarantees the right to privacy of correspondence and other means of communication of every citizen of Bangladesh, subject to certain qualified restrictions. This highly progressive and visionary provision of the Constitution codified a crucial fundamental right which, in an era of burgeoning data proliferation and exponential growth in connectivity, driven largely by the visionary policies and initiatives adopted and implemented by the Government of Bangladesh ("**GoB**"), has become all-important and a stimulus for legislative activism in the area of data privacy and security.

The Digital Security Act 2018 ("**DSA 2018**"), in overhauling the Information and Communication Technology Act 2006, introduced provisions that afford protection to the identity information of individuals. Section 26 of the DSA 2018 prohibits the collection, sale, possession, provisioning, or use of identity information of another person without lawful authority. However, these provisions are manifestly inadequate to address the multifaceted data privacy and security concerns and challenges faced by individuals and businesses. Hence, we commend the timely initiative of the GoB in drafting the Information Privacy and Security Rules 2019 ("**Privacy Rules**") to be issued under the DSA 2018, which, if enacted, would be the first substantive legal and regulatory framework on data privacy and security in Bangladesh.

This submission sets out the key issues in the current draft of the Privacy Rules together with recommendations based on an international benchmark of privacy laws. The benchmark is primarily based on the European Union's General Data Protection Regulation ("**GDPR**") and other international benchmarks, such as the APEC Privacy Framework and the OECD Privacy Principles. We refer to these together as the "**International Benchmarks**".

Generally, the draft Privacy Rules appear to be inconsistent, inexplicit, and generally inadequate to address the contemporary data security concerns and would benefit from harmonization with globally accepted standards provided in the International Benchmarks. This would be consistent with the aims of the ASEAN Framework on Digital Data Governance and the work of the ASEAN Regional Forum. We believe further amendments to the draft Privacy Rules are necessary before these are published in the official Gazette.

Aspects of the draft Privacy Rules which are of most concern include:

- extraterritoriality provisions which create an unduly broad territorial scope;
- extensive use of undefined terms and expressions, which creates ambiguity and unpredictability, including the definitions of "data processor" and "sensitive personal information" which are out of step within International Benchmarks;
- unclear and duplicative provisions relating to consent and notice requirements; and
- age of digital consent not in line with globally accepted standards and practices.

Additionally, the draft Privacy Rules do not expand upon or clarify the existing issues with Section 26 of the DSA 2018, namely the expression "without any legal authority", which remains undefined. In the absence of guidance, this provision has potential for broad interpretation and therefore should be defined subject to sufficient qualification, exceptions or exemptions so as to avoid frivolous and vexatious claims. For example, Section 26 should not extend to collection or possession of identity information available in public domain or

where exercising the fundamental right to freedom of speech expression, freedom of the press, or freedom to conduct any lawful trade or business.

In order to promote the growth of the digital economy, and to participate effectively as part of the global digital ecosystem, Bangladesh requires a legal framework that is aligned with global standards and best practices; provides industry, consumers and the GoB alike the ability to operate within a clear, predictable, balanced and stable legal environment; and promotes good data governance and enhances confidence. Without effective data privacy and security regulation and policy, the growth of digitalisation, e-governance, e-commerce, innovation and the economy of Bangladesh in general may be stymied in the near future. Against this backdrop, we would like to take this opportunity to provide our comments and suggestions in relation to the draft Privacy Rules.

B. **Detailed comments and recommendations on the provisions in the draft Privacy Rules are as follows:**

a. **Extra-territoriality**, *Rules 3(1)(b) and (c)*
The Privacy Rules are intended to apply to all those that "carry out information processing activities within the territory of Bangladesh or any place outside the borders of Bangladesh", including to those that are "not registered as a commercial entity in Bangladesh…and [do] not supply goods within Bangladesh". The extraterritorial scope of the Privacy Rules is unduly broad and effectively covers every entity worldwide that processes personal information. There is no requirement of a nexus with Bangladesh for the Rules to apply, which is unusual and out of step with the International Benchmarks.

While it is important to ensure the robust protection of data privacy of persons within Bangladesh, unfettered extraterritorial scope will be practically difficult to enforce, will create conflict of law issues and not aligned with both national and international approaches to territorial scope (noting that Section 4 of the DSA 2018 requires that an offence committed outside Bangladesh must also be an offence recognised by the DSA 2018 or must have nexus to Bangladesh to be actionable). The application of the Privacy Rules should be confined to data controllers and processors established within Bangladesh. If extra-territoriality must be retained, then this should be aligned with Recital 23 and Article 3 of the GDPR which imposes a minimum threshold on entities located outside the jurisdiction before they must comply (i.e. where the entity is actually offering goods or services to data subjects in the jurisdiction, or monitoring their behaviour).

b. **Definition of "data processor"**, *Rule 2(e)*
"Data processor" is defined to include employees of a data regulator (akin to the concept of a data controller) as well as "independent processor operating under any personal data regulator". However, inclusion of a data regulator's (data controller's) employees under the definition of a "data processor" does not align with International Benchmarks.Employees processing personal data within an organisation are generally considered as doing so to fulfil the organisation's tasks as data controller and would not be classified as a "data processor" separate from the organisation in question. This imposes unnecessary direct obligations on each employee. For example, Rule 14(2) imposes a requirement for data processors to take appropriate security measures to protect the information in their custody. This therefore imposes direct obligations on each individual employee who handles personal information on behalf of their employer to secure the data, which is out of step with international practice. Such security measures should be the responsibility of the data controller/employer. Imposing direct obligations on employees is onerous and may result in a reduced willingness for global companies to operate in Bangladesh.Accordingly, employees should be omitted from the definition of "data processor". The terms ‘data regulator’ and ‘data processor’ should be defined clearly, so as to prevent any confusion about the scope of the term. There is no need to use the term ‘personal data regulator’ separately, as it will be covered within the definition of a ‘information regulator’. (i) The definition of the term ‘organization’ can be removed. All entities will get covered within the definitions of ‘information

regulator' and 'data processor'. The use of these terms is also consistent with the group. The definition of an 'information regulator' (also known as a 'data controller') and data processor can be taken from existing data protection laws in other countries, such as the European Union's General Data Protection Regulation ("**EU GDPR**"). This will ensure consistency in the definition of these terms across laws of different countries, making it easier for foreign companies to comply with the Rules.

Thus, we recommend that- (a) define the expressions 'data/information regulator' and 'data processor' clearly, referring to their definition in the EU GDPR; (b) remove the definition of the term 'organization'.

c. **Definition of Personal Information**

The definition of personal information might be framed as: "information reasonably linkable to an identifiable individual or to a device associated with an identifiable individual and does not include:

- Anonymized information
- Aggregated information
- Pseudonymized information
- Employee data
- Public information, which includes information which a person makes public
- Generated information"

d. **Sensitive personal information**, *Rules 4, 7 and 20*

The definition of "sensitive personal information" includes ethnic origin, political or religious views. This is not included within GDPRs definition of 'sensitive personal data'. Inclusion of this category, is impractical and may have a deleterious effect. Few concerns to note are:

- This could have a chilling effect if this is applicable to online videos uploaded on platforms where people might express religious or political views as part of their content. Requiring additional conditions on processing this data could result in lower quality experiences for users and barriers to free expression.
- For electoral purposes, the political affiliation of the candidate is publicly available which allows a voter to choose the person/ party for which he may want to cast the vote.
- The religious and/or political beliefs or affiliations of almost all data subjects that are public figures are already publicly available. In fact, such beliefs/ affiliations of individuals are subject to changes and there might not be any way for a data fiduciary to accurately identify them.

The definition also includes passwords and bank account or credit/debit card or other payment instrument details or records of financial transactions. "Sensitive personal information" also includes in sub-rules 8 and 9 the "details provided by an organization" regarding the categories of data listed and "any information [listed] taken by enforcement agency for preservation or processing" (however it is unclear how these are different from the categories listed in (1) to (7)). The definition of sensitive personal information should be aligned with Article 9 of the GDPR - it should encompass personal information should actually be more sensitive and of a higher risk to individual privacy and not include, for example, passwords, and financial transaction data. Not all types of financial transaction 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. Also, to assess loan applicants and prevent fraudulent transactions, fintech lenders source customer data from trading and brokerage accounts, and credit and debit card transactions directly from banks or from Credit Agencies, the latter being private parties (CRAB in Bangladesh). Similarly, all passwords are not equally sensitive – it would not be proportionate to require more

stringent processing requirements to apply equally to a person's streaming video account log in as well as to the account details to their online health records. The definition of "biometric information" should be clarified to replace "help identify" with " that uniquely identifies".

Rule 20(1) states that sensitive personal information may not be collected or processed unless express consent is obtained via letter, fax, email, or in writing. There are some exceptions for government agencies, NGOs and other entities where this is required by law. While requiring express consent for sensitive personal information is broadly aligned with the International Benchmarks, the overly prescriptive means through which such consent must be obtained is not. It should be incumbent upon the data regulator to demonstrate that the data subject has given consent and facilitate the provision of that consent in a way which is appropriate to the service offering and the user experience.

Rule 20(4) requires data regulators and data processors to be responsible for ensuring that sensitive personal information is subject to enhanced security measures. However, organisations should be permitted to ensure that the manner in which consent is obtained is appropriate. Furthermore, the law should be technology-neutral to future-proof against other technologies that may not yet be available, but which may be more effective for obtaining requisite consent. This requirement appears to take inspiration from a similar one under India's Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011. However, it should be flagged that under India's new Personal Data Protection Bill that was tabled in parliament last year, the requirement for consent to be obtained via letter, far, email or in writing has since been removed. Further, the obligation on data processors to implement security safeguards, mitigate risk of security breach and even to take measures to reduce damage is at odds with the role of a data processor, which is to process PI based on the instructions of, and on behalf of a data regulator. Data processors do not have visibility over the nature, scope and purpose of processing of such PI, and are unable to ascertain the likelihood of harm. Data processors are therefore unable to make an assessment of security standards necessary for such processing. Therefore, the responsibility for determining and implementing security safeguards, mitigating risks and taking measures to reduce the damage should vest solely with the data regulator and should not be extended to data processors. Further, as per the terms of the agreement between the data regulator and data processor, the data regulator can always direct the data processor to implement appropriate security standards and this could serve as an effective way to address the problem.

We therefore recommend that the references to data processors should be removed from Rules 14(2), 27, 28, 31 and 37(1).

Rule 7 states that "each person shall have the final power to determine the method of distribution for the purpose of rule 4". It is not clear what intention behind this rule is and whether this means that data subjects should have a right to stop or withdraw consent to any processing of their sensitive personal information. This also undermines the requirement for data subjects to give consent prior to the collection or processing of their sensitive personal information, suggesting that this is not "true" consent since Rule 7 implies that organizations would otherwise determine the method of disclosure of such data. This provision should be revised to eliminate the resulting uncertainty for organisations as to whether they can rely on consent from data subjects and the extent to which an organisation can disclose such data.

e. **Grounds for Processing of SPI,** *Rule 20*

The requirement to process SPI only pursuant to the information provider's express and written consent is restrictive. Further, consent does not absolutely guarantee that information provider's interests will be protected and instead can create "consent fatigue" for organizations and data subjects as mentioned above. In many circumstances, it may be impractical or unnecessary to obtain express consent. The

GDPR recognizes other grounds of processing of SPI and we recommend that Rule 20 be revised to allow for processing of SPI on such grounds other than based on consent- (i) for employment, social security and social protection purposes; (ii) where processing is necessary for the public interest; (iii) where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and (iv) where processing is carried out in the course of legitimate activities with appropriate safeguards by the entity. Further, all exemptions from processing of PI for specified purposes as set out in Rule 19, should be extended to include SPI that is processed for similar purposes.

The requirement to process SPI only pursuant to the information provider's express and written consent is restrictive. Further, consent does not absolutely guarantee that information provider's interests will be protected and instead can create "consent fatigue" for organizations and data subjects as mentioned above. In many circumstances, it may be impractical or unnecessary to obtain express consent.

The GDPR recognizes other grounds of processing of SPI and we recommend that Rule 20 be revised to allow for processing of SPI on such grounds other than based on consent- (i) for employment, social security and social protection purposes; (ii) where processing is necessary for the public interest; (iii) where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and (iv) where processing is carried out in the course of legitimate activities with appropriate safeguards by the entity.

Further, all exemptions from processing of PI for specified purposes as set out in Rule 19, should be extended to include SPI that is processed for similar purposes.

Rule 20(3) also states that SPI collected by an entity may be 'examined' under certain circumstances. However, the meaning of 'examination' is unclear and will create significant regulatory uncertainty. The meaning and standards of examination should therefore be clarified.

We therefore recommend that seeking explicit consent should be made as one of the grounds for processing SPI under Rule 19, rather than the only ground. We also recommend expanding the grounds for processing of SPI by borrowing certain grounds from GDPR. Further, all exemptions from processing of PI for specified purposes should apply to SPI as well.

We also recommend that the meaning and standards of examination of profiling under the rule should be clarified.

f. **Consent and notification ("confidential notice")**, *Rules 6(2), 6(3), 6(4), 8, 16, 18, 19 Schedule II*

1. Consent: There appears to be a general obligation in Rule 6 to only collect, use or process personal information where consent has been obtained (there are limited exceptions for emergency situations and national security in Rules 6(4) and 15). This consent must be independently-given.

   Rule 19 also sets out what appears to be further exceptions to the consent requirement (i.e. where the personal information is necessary for the execution of a contract, to perform a legal obligation or for emergency treatment). However, the translated text states that consent *is* required for these situations, which is counterintuitive. Rule 19 should clarify the situations where consent is not required to collect and process personal information. These exceptions to consent should align with the alternative lawful bases of processing under the GDPR, and

should include at minimum a “legitimate interest” or “public interest” basis of processing. Other International Benchmark jurisdictions such as Singapore have indicated that they intend to include “legitimate interests” as an additional basis of processing precisely because where there is a relevant and appropriate relationship between the data subject and the data regulator, the processing of data is line with user expectations and respects the interests of the user.

Rule 19 should ideally state that consent for collection and processing of data should ***not*** be required in the circumstances mentioned in the rule. ‘Consent’ cannot be the sole basis for processing of PI or data, as it can create hindrances in situations where the data needs to be processed urgently. Additionally, it can also result in consent fatigue for organizations and information providers.

Consent fatigue is a well-recognized phenomenon where data principals feel harassed by constant notices that seek consent, and are therefore likely to reduce the use and adoption of digital services. Alternatively, they are likely to simply accede to consent request, thereby rendering it meaningless. This would have a cascading impact on existing business models in marketing, consulting, fintech and on the adoption of new technologies such as artificial intelligence or AI. This would ultimately impede innovation and economic development in Bangladesh, as these industries will likely migrate to countries with favorable consent regimes.

Rule 19 should clarify the situations where consent is not required to collect and process PI. These exceptions to consent should align with the alternative lawful bases of processing under the GDPR, and should include at minimum a "legitimate interest" and performance of contract for processing data without consent. Both legitimate interests and performance of a contract form standard legal bases for processing of data in the GDPR. The GDPR does not call for prior consent before undertaking such processing. This should be recognized under Rule 19 because obtaining valid, meaningful, and informed consent of data principals for every processing activity is technically onerous, and likely to impair the user interface and experience, without enhancing data protection outcomes.

We therefore recommend that Rule 19 should be revised to: (i) remove consent as a prerequisite; and (ii) expand the grounds for processing by adding ‘legitimate interest’ and performance of contract.

2. Notice: Rules 8, 16 and 18 contain overlapping requirements on the notice that must be provided to data subjects. Broadly, before collecting or processing personal information, organisations must provide data subjects with a "confidential notice" containing the information set out in Schedule II (both in English and in Bengali). The "confidential notice" must be unbundled and easy-to-understand. All notice requirements should be consolidated and overlapping provisions removed. Further, clarification is needed around why the notice to be provided is a "confidential" notice, as opposed to established data protection regimes across the world, none of which include such a requirement. Additionally, the detailed notice requirements in Schedule II are too prescriptive and may result in notice-fatigue for data subjects given the amount of detail that must be provided in Schedule II for each collection of personal information. Streamlining this to only include the types of personal information and purposes of processing would allow organisations greater flexibility on how the notice should be presented to individuals. For expanded grounds of processing data other than consent, please see our comments on rule 19.

g. **Notice and Consent Requirement**, *Rule 24*

This rule requires the data regulator to notify the user and take her written consent before transferring her data to a third party. This requirement is already covered under rule 21(a) of the Rules. **Thus, we recommend that rule 24 should be merged with rule 21.**

h. **Method of distribution**, *Rule 7*

This rule allows the information provider to determine the final manner and method of distribution of their sensitive personal information. (i) Allowing every information provider the right to decide the method of providing their sensitive personal information ("**SPI**") will be a costly, and in some cases, a commercially impracticable exercise for multinational service providers, which will deter them from providing services in Bangladesh. The flexibility to choose the method of providing sensitive personal information should be left at the discretion of the relevant Service Provider, subject to applicable security standards. Further, if the information providers are not comfortable with such method, they can always withdraw such consent provided to the Service Provider in accordance with the Rules.

i. Such a right of determining the method of providing SPI is not provided to the information provider in most data privacy legislations around the world. Even mature jurisdictions such as the European Union ("**EU**"), which introduced the General data Protection Regulation ("**GDPR**") only prescribe that the manner in which one's personal information is collected should be lawful and necessary for the purpose of collection. The GDPR is currently the most comprehensive and widely followed data protection legislation in the world and it does not touch upon giving the information provider the right to decide the manner of providing their SPI. Several multinational corporations having business presence throughout the world, including that in Bangladesh, are already compliant with the requirements under the GDPR. The Rules should therefore apply similar standards so that higher efficiency is achieved with minimal costs, which will further incentivize and attract businesses to Bangladesh.

Rule 7 should be amended to clarify the purpose it seeks to achieve while at the same time, aligned with the language in other privacy legislations. Alternatively, it should be deleted.

j. **Disclosure of personal information**, *Rules 21, 24*

The Privacy Rules provide that personal information may only be disclosed to a third party where the data subject has provided written consent, where it is necessary pursuant to a contract between the recipient and data subject and where the recipient complies with the Rules. These disclosure requirements are onerous and unusual. Organizations often need to disclose personal information to service providers and other third parties to provide their products and services and to operate. This is entirely compatible with the purposes of the data processing. Further, these requirements do not align with general business practices or with International Benchmarks . The Privacy Rules should be amended to permit disclosure to third parties as long as it is compatible with the original purpose. This balances individual privacy with business efficiency.

k. **Data breach notification**, *Rules 13, 27, 31*

There is a general requirement in Rule 13 for information providers (data subjects) to be notified of the "danger/risk" of a personal information breach within 7 days. There is also a requirement in Rule 27 for a data regulator and data processor to notify both the Agency and the information providers (data subjects) of any general data (more broadly defined than personal information, as discussed above) breach of the same within 7 days. There is a further overlapping requirement in Rule 31 for data regulators, data processors and all third parties to notify those affected by data breaches caused by "cyber attacks" within 7 days. It is unclear if "cyber attacks" are the same as "cyber incidents" defined in Rule 2(o).

The three different provisions covering data breach notifications are overlapping and should be streamlined and consolidated for clarity. Requiring notification to data subjects and the regulator for every data breach may result in notification fatigue for data subjects and an undue administrative burden for regulators. This would de-sensitise data subjects to the impact of such breaches and would not allow the regulator to allocate appropriate responses to investigating and addressing harmful breaches. Accordingly, a minimum threshold aligned with International Benchmarks (including Australia, Singapore, Philippines, and under the GDPR) should be introduced before a breach becomes notifiable, for example a requirement that a data breach is likely to cause serious harm to affected individuals. Therefore the recommendation is that the data fiduciaries should be allowed to decide on the materiality of the breach and accordingly report to the Agency or at best certain threshold (like quantum of users affected) can be prescribed when such breach needs to be notified to the Agency. It would also be beneficial to allow for more flexibility in the timeline for reporting because, while timely notification is important, it is more important that organisations are able to present the facts fully and accurately and focus on breach mitigation. A prescriptive 7 day timeline may not always be appropriate – this could be too long for very harmful breaches, and too short in some cases where further investigation is required. Notification should not be required for disclosures or breaches if the data is encrypted or anonymised; does not cause or is not likely to cause any harm to the user; is a result of employee access in good faith and if the data is not further disclosed; the data is in public records.

Further, (i) However, it would not be appropriate for data processors to be obliged to notify the in the event of data breaches. Data processors may not have visibility over the content of PI of data regulators, meaning that they would not be able to distinguish between an intentional movement of data or a security incident, let alone whether a data breach involves PI. Finally, data processors do not have direct relationships with the information providers and would therefore not be able to meaningfully or effectively communicate matters relating to a data breach with them. Therefore, data processors should have the responsibility to notify data regulators of confirmed data breaches, in a reasonable timeframe, given the specific circumstances, and in accordance with their contractual agreements. The responsibility of notifying affected information provider or the concerned authorities should therefore ultimately reside with the data regulator. Data processors are also unaware of the data regulator's intentions towards the treatment of data such as decision to make certain categories of data public. Also, the parties frequently agree that data processors should have only limited access to data regulators' data, which hampers data processors' ability to know whether a breach has occurred. Further, even under the GDPR, a data processor is only required to notify the controller without undue delay upon becoming aware of a breach. The GDPR does not mandate the processor to adhere to the same requirements as the controller. This is more aligned with the practical realities of a data processor's role. Additionally, mandating both the data regulator and the processor to report breaches could result in erroneous or conflicting reporting of breach which could hamper remediation efforts.

We therefore recommend that the references to data processors should be removed from Rules 14(2), 27, 28, 31 and 37(1) and should only be limited to data regulators. We also recommend that Rules 27 and 31 be amended to mandate a data processor to report a PI breach to data regulator only upon confirming the breach itself.

l. **Transition period**, *Rule 1(2)*

The Privacy Rules are intended to come into effect immediately following publication in the official Gazette. The lack of a transition period for organisations to comply with the Privacy Rules is not practical and may result in widespread non-compliance at the start due to a lack of awareness. Allowing a transition period of at least 18 months will enable organisations to put in place systems and procedures to enable compliance with the new laws. Other International Benchmarks also had appropriate transition

periods to allow organizations to comply – for example, the GDPR had a 2 year transition period, Singapore had about 18 months and Thailand originally had a transition period of 1 year before the enacted law took effect (now pushed back to 2 years). The government can also consider phased implementation of the provisions of the Act (once notified).

m. **Definition of "processing"**, *Rule 2(h)*
"Processing" is defined as "recording of information or the receipt of information or the unique management of a data management operation, adaptation or change of information, retrieval of information, use of advice or information, broadcasting or otherwise publishing, combining, blocking and deleting or destroying any other information". While the spirit of this definition seems broadly aligned with that in the International Benchmarks such as Singapore's PDPA and the GDPR, there are some unusual inclusions such as "use of advice" and "unique management of a data management operation" which are vague, undefined, and do not align with the typical definitions of "processing". This definition should be amended to align with the definition of processing under Article 4 of the GDPR.

n. **Requirement to formulate and make policies for data**, *Rules 2(c) and 5*
Organisations must put in place "policies for collecting, receiving, storing and managing *data*". These policies must be published on the organization's website and be available for information providers (data subjects) to access. The policies should also set out the purpose of collection and use of the data and the security measures taken to protect the data.

The policies that must be put in place appear to encompass more than just personal information. "Data" is defined separately from "personal information" in Rule 2 and means any "formally prepared information, knowledge, facts, concepts or instructions that has been processed, or 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 cards, punch tape, or which is stored internally in a computer's memory". As such, the policies to be issued are both wider (in terms of the inclusion of non-personal information) and narrower (since they only relate to formally prepared data on a computer network or system) than that usually required by other International Benchmarks. As currently drafted, there is some ambiguity as to what will constitute data (e.g., it is unclear if anonymized, aggregated, unprocessed or raw data fall within this definition). While having general data policies is important for any organization, there is limited benefit to making these available to data subjects since non-personal information has limited privacy impact for them. This obligation should only apply in respect of "personal information", in line with the requirements of other International Benchmarks.

o. **Protection of personal information**, *Rules 28 and 37*
The relationship between the provisions in Rules 28 and 37 is not entirely clear. Rule 28 requires organizations to implement appropriate security measures in consultation with the Agency and in accordance with the "manner and nature of security prescribed in government notifications". The requirement to consult with the Digital Security Agency is onerous and would result in an undue administrative burden for both organisations and the Agency. This consultation requirement would extend the time required for a business to comply with the Rules and could thus impact Bangladesh's attractiveness to both local and global businesses wishing to establish privacy-compliant operations. Furthermore, it is unclear what metrics the Agency will use to assess these measures, and the extent of the Agency's involvement in designing these measures. Further, what constitutes maintenance of "reasonable security "under Rule 37 is ambiguous and indeterminate. For instance, the concepts of "security measures", "detailed information security program" and "actual security" are not clearly described and terminology is inconsistent (variously referring to agency / company / person etc).

The prescriptive security standards in both Rules 28 and 37 are arbitrary and increase compliance costs for organizations. For example, Rule 37 prescribes “IS / ISO / IEC 27001” as the requisite standard, but also it leaves open for the Agency to issue Standard Operating Procedure and for the GoB to set the standards and criteria from time to time, which would create compliance issues for the businesses. The measures taken to protect personal data should be proportionate to the nature of the personal data and the types and purposes of processing. There is no "one-size-fits-all" solution. For example, a small store running a simple membership loyalty programme cannot be expected to implement the same security controls to protect the personal data it collects as a healthcare company that deals with thousands of patient records every day.

Rule 37 also requires the “data collection and processing company” to arrange an annual audit by an auditor appointed by the GoB, with the audit report to be sent to the Agency who may issue instructions.The frequency, nature and the standard of audit is not specified. Data processors do not have visibility over the nature, scope and purpose of processing of data. Data processors are therefore unable to make an assessment of security standards necessary for such processing. Therefore, the responsibility for determining and implementing security safeguards should be vested solely with the data regulator and should not be extended to data processors.

Further, the requirement to undergo an annual audit is a costly and unnecessary measure. It should be left to the processors to demonstrate through mechanisms commensurate with the information handled by them that they follow reasonable security practices.

Given the above, we recommend deleting Rule 37(2) and allowing data regulators to demonstrate their compliance using reasonable and appropriate means, such as through internal reviews of their security controls. Alternatively, instead of a mandatory requirement, the rules can provide for voluntary adoption of internationally recognized standards for security, including ISO 27018 and APEC CBPR. This obligation will be onerous for organisations and the Agency alike and should be reconsidered

p. **Data subject rights**, *Rules 9, 10, 11 and 12*

1. Access (Rule 9): Each person has a right to access their personal information and receive a copy "in accordance with Schedule II". However,Schedule II refers to the notice requirements therefore it is unclear what the intention behind this is provision and it should be removed.

2. Correction (Rule 10): Each person has the right to correct their personal information where it is unclear or incomplete. Amendments must be made by the data controller as prescribed by the government and completed within 60 days of the request. Given the varying structures of all organizations that will be subject to the Privacy Rules, requiring both small and larger companies to comply with the same correction process (regardless of resourcing) would not be appropriate. The 60 day timeframe is also overly prescriptive and should be more flexible. Inspiration can be taken from Singapore's PDPA which permits a longer response time as long as the data subject is notified within 30 days of when the request will be fulfilled. Read with Rule 32, an onerous obligation is sought to be imposed on data regulators, processors and third parties to ensure accuracy of the information. Traditionally, data controllers and processors are absolved of such obligations, which are instead framed to only to empower data subjects to take steps to have their information corrected, or updated, as applicable. Notably, Rule 10 (3) uses the terms ‘data manager’, which remains undefined and requires harmonisation, as explained in point o below.

Further, under this rule, a data processor may be required to implement an information provider's request to make amendments to their personal information ("PI") where it is unclear or incomplete. However, this is a function that can only be performed by data regulators and not processors.

Data processors operate under data regulators. Data regulators are the entities who determine the process of using or applying PI. Data processors do not usually have a relationship with information providers. They are typically not in a position to make meaningful or independent decisions about the processing of PI either. Hence, data processors cannot be responsible for amending information provider's PI based on requests received from information providers.

Data processors may not have necessary control over networks and data to make such corrections or changes in any case. Data processors are also bound by their employer-employee relationship or contract to follow the instructions of the data regulators, which may also impede their ability to make such amendments.

Therefore, this rule should be amended to clarify that the responsibility to rectify or correct the PI of information providers must lie with data regulators and not data processors.

Additionally, this rule does not provide the data regulator with the power to reject an information provider's request for correction of their PI, where such request is untenable or where they may be adequate justification for denying such request. The data regulator can be required to explain the reason for denying the request in writing to the information provider.

We therefore recommend that Rule 10(2) should be revised to: (i) remove references to data processors; and (ii) data regulator should be provided with power to reject users' request for correction of their PI, when there is adequate justification in the reasonable opinion of the data regulator for denying such request.

3. Deletion (Rule 11): The information regulator (data controller) must delete personal information where the purpose has been fulfilled, consent has been withdrawn, it was collected illegally, or it has been ordered by a court. There are limited exceptions. This right should be consolidated with the requirements on retention of personal information and that further exceptions to this deletion requirement be introduced (see paragraph 'o' below).

4. Data portability (Rule 12): Each person has the right to obtain the personal information they have provided in a commonly used and machine readable format and the means of transferring the personal information they have provided to another data controller. This data portability requirement should be limited to only downloading the information. Requiring data controllers to also share the data with other data controllers will create additional operational costs in communicating and transferring data. It would be more effective if the data subject were responsible for transferring this data instead and the privacy concerns would be sufficiently addressed by the ability to download the data. Rule 12 should include exceptions if giving effect to this right would:
    - disclose trade secrets or proprietary info;
    - compromise privacy, security or integrity;
    - be infeasible on technical grounds or require disproportionate effort;
    - require re-identifying or otherwise linking information that is not presently considered personal information;

- interfere with law enforcement, judicial proceedings, investigations;
- undermine efforts to guard against, detect, or investigate malicious, unlawful, or fraudulent activity or enforce contracts; or
- violate laws or the rights of others.

q. **Data protection officer**, *Rule 33*

Each data regulator, data processor and third party must appoint a DPO, who must have technical expertise related to data protection. This requirement is extremely broad, in light of the expansive extraterritorial scope in the Privacy Rules. It effectively requires every single organization globally to appoint a DPO. In addition to limiting the extraterritorial scope of the Privacy Rules, it would be valuable to introduce minimum thresholds before the DPO must be appointed, similar to that under Article 37 of the GDPR. For example, 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 that consist of processing on a large scale of sensitive personal information should be required to appoint a DPO.

r. **Consent and Notice Obligations**, *Rules 17 and 18*

It would not be appropriate for data processors to be obligated to verify the consent and inform/ give notice to every information provider regarding the details of the information being collected. Data processors do not have a direct relationship with information providers. They do not always have visibility over the data being collected either and merely operate under the instructions of the data regulators. They, therefore, cannot be tasked with the onerous obligation of verifying the information. For the same reason they would therefore not be able to meaningfully or effectively communicate to information providers the information on the data being collected, the purpose of collection etc.

We therefore recommend that Rules 17(1) and 18(1) be amended to remove the references to data processors.

s. **Parental consent required for individuals under 18**, *Rule 17*

The draft Privacy Rules require consent to the personal information of a minor: (i) shall be obtained from a legal guardian; and (ii) be duly verified by the data regulator and data processor. Presumably this is a reference to consent to collection, control, processing, storage and disclosure, per Rule 16. Rule 17 prescribes 18 years of ages as the age of majority in accordance with the Majority Act, 1875.

Given the extent of access to internet and technology in the increasingly globalized world, setting of 18 years of age as the digital age of consent in the draft Privacy Rules is inconsistent with global standards. There is a considerable body of evidence internationally that points to 13 as the appropriate age at which parental consent should not be required to access the services of information society providers. For example, the Irish Ombudsman for Children and the Internet Safety Advisory Committee has recommended a digital age of consent of 13 years, which was supported by the Irish Special Rapporteur on Child Protection, the Irish Society for the Prevention of Cruelty to Children and the Irish Children's Rights Alliance, which represents more than 100 organizations involved in child welfare. Additionally, the Singapore Personal Data Protection Commission has determined that it generally considers children over the age of 13 to have sufficient understanding to be able to consent on their own behalf. Further, in the United States of America, parental consent is required for children under the age of 13. In keeping with international best practice and generally accepted practice, the digital age of consent should be set between 13 and 16, as is provided for under the GDPR.

t. **Definition of "information regulator" / "data regulator"**, *Rule 2(d)*
"Information regulator" is defined as "a person who, singly or jointly, or in coordination with another person, determines the process of using or applying personal information". This term aligns with the general concept of a data controller in the International Benchmarks, such as the GDPR. However, the term is used only 4 times in the Privacy Rules, whereas the undefined term "data regulator" is also used more commonly throughout the document, apart from use of the term "data manager." The distinction between "information regulator" and "data regulator" (if any) needs to be clarified and the appropriate term used consistently throughout. GoB may, in any event, wish to consider adopting the term "data controller" for consistency with other International Benchmarks (noting this term is used 3 times in the English translation of the Privacy Rules).

u. **Retention of personal information**, *Rules 22 and 23*
These provisions contain overlapping obligations relating to the retention of personal information, but broadly, they require that personal information must not be retained once the purpose has been fulfilled and must then be destroyed immediately, unless the data subject has consented to storage for a longer period of time or it is required for historical, statistical or research work. In order to align with International Benchmarks, this obligation should take a more realistic and reasonable approach by allowing for expeditious deletion of data and should incorporate further exceptions to the retention limitation requirement, such as where required for "legal and business purposes" as provided under Singapore's PDPA.

v. **Cross-border transfers of personal information**, *Rule 25*
The Rules should clarify that consent is one basis for transfer but is not required for all transfers, in line with the APEC Cross Border Privacy Rules Framework and OECD Privacy Principles. Under those frameworks, data transfers are permitted as long as the data regulator remains accountable for protecting the data regardless of geographic location.

The free movement of data underpins the digital economy and plays a fundamental role in ensuring data-driven growth and innovation. The effective and efficient functioning of data processing across borders is a fundamental building block in any data value chain. Hence, consent should be made only one of the several grounds for such transfer.

Allowing for cross border transfer of data is essential for aiding in international technology transfer processes and to ensure that Bangladesh's growth and potential is met from a technological standpoint.

This rule should be aligned with international practices such as GDPR to aid in smooth running of businesses across borders. Article 46 read with Article 49 of the GDPR provide the circumstances in which the EU permits transfer of information outside the EU region, which is broader in scope when contrasted with the Rules.

Under these provisions, the option to transfer information is available not only where the information provider has provided explicit consent, but also in situations such as where the transfer is necessary for performance of a contract in the interests of the data principal, to protect the data principal's interests or for defence of legal claims, etc. The Rules should attempt to maintain a similar standard as the GDPR as this would take into account the practical considerations of businesses while ensuring that adequate protection of PI is maintained.

Accordingly, the grounds for transferring PI and SPI offshore should be expanded as follows:

1. Legally binding enforceable instruments: These are commonly deployed legal solutions, designed to enable data transfers between countries by ensuring adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.
2. Standard contractual clauses: These are ready-made rules that provide for data transfers to third-parties located in other countries. The clauses, which are to be used in contracts, are developed by the DPA, and, as such, are automatically considered to provide sufficient safeguards for transferring data, even to countries that do not enjoy an equivalence or adequacy recognition.
3. Protective measures: If the data regulator demonstrates that it has taken such reasonable steps such as ensuring that:

    - the overseas data recipient is bound by comparable obligations under their applicable laws;
    - there is an appropriate safeguard of PI in the recipient's jurisdiction;
    - the transfer is necessary in order to protect the vital interests of the data subject; or
    - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject.

The Rules should leverage international data transfer standards and contracts to ensure interoperability with global standards (the APEC Cross-Border Privacy Rules offer a multilateral cross-border data transfer framework that Bangladesh can consider joining). An example would be Article 24 of Japan's APPI, which imposes restrictions on the transfer of personal information of Japanese citizens to third parties in foreign countries except when a third party has established a system which meets the Rules of the Commission to "continuously implement equivalent necessary measures." These regulations for implementing Article 24 specifically call out a company's APEC Cross Border Privacy Rules (CBPR) certification as satisfying this requirement.

The Rules should also include certifications as mechanisms for ensuring that data is transferred in accordance with high privacy standards. Under such an approach, a data controller that demonstrates to an independent third party certifier that it complies with specific requirements should be allowed to transfer data outside of Bangladesh without consent of the individual or by relying on another method.

w. **Cyber incidents and disclosure to govt agencies**, *Rule 2(o)*

"Cyber incident" is defined as "the actual or alarming hostile situation regarding cyber security where unauthorized access is established in violation of security measures and protocols, where any service is stopped or interrupted and any data is changed, processed and collected through unauthorized use of computers and computer systems." This definition is unclear. What amounts to an "actual or alarming hostile situation" is vague and the need for services to be stopped or interrupted is not always reflective of the severity of a cyber incident. The only use of "cyber incident" in the Privacy Rules is in Rule 21(b) which requires organizations to hand over personal information to government agencies (without data subject consent) where it is required to prevent a cyber incident. Ideally, the intention behind this and how it differs from a data breach should be clarified. If this concept is retained as distinct from that of a data breach, we would recommend adopting a harm-based approach which requires the relevant situation to have met the threshold of causing serious harm to an individual before it will be considered to be a "cyber incident" for the purposes of the Privacy Rules.

x. **Allocation of Liability between data regulators and data processors, Rules 29,30,32,33**

These rules impose several obligations on data regulators as well as data processors such as satisfying legal privacy obligations, breach notification requirements, appointing data protection officers, and transparency requirements.

The Rules should clearly demarcate the roles and responsibilities of data regulators (who determine the means and purposes of processing PI) and those of data processors (who process data on behalf of controllers). Data regulators should bear primary responsibility for satisfying legal privacy obligations, breach notification requirements, appointing data protection officers, and transparency requirements. By contrast, data processors should be responsible only for following the data regulator's instructions pursuant to their contractual agreements.

The obligations under Rule 20(4), 29, 30, 32 and 33 should be applicable to data regulators alone, and not to data processors, who only process PI on behalf of the data regulators. This is because data processors only process data on the instruction of a data regulator and are involved in the processing activity on the basis of the instructions provided to the data processor. It is unreasonable to hold data processors responsible for such activities as they do not have insight into the type of data that is stored or processed using their services. The conditions of satisfying legal privacy obligations, breach notification requirements, appointing data protection officers, and transparency requirements should be imposed on data regulators and imposing such obligations on data processors will ultimately result in increase in cost of services.

Further, data processors do not have visibility over the nature, scope and purpose of processing of such data, and are unable to ascertain the likelihood of harm. Data processors are therefore unable to make an assessment of security standards necessary for such processing. Therefore, the responsibility for determining and implementing security safeguards should be vested solely with the data regulator and should not be extended to data processors. Additionally, since the relationship between data regulators and data processors is contractual and data processors will not have the right to make determination with respect to a breach and report it. Further, data processors should not be held responsible for the failure of data regulators to meet their obligations.

We therefore recommend that these rules should be revised to remove reference to data processors.

y. **Transfers to third parties**, *Rule 21*

Under this rule, PI can be transferred to a third party under the following grounds: (a) consent of the data subject; (b) third party complies with the Rules; and (c) transfer is effected under an agreement. Additionally, rule 21(b) allows personal information to be transferred to government agencies, including the Digital Security Agency, without prior permission. Specifically, the data processor will receive a letter from the Digital Security Agency explaining the reasons for seeking information.

Consent cannot be the sole basis for processing of PI, as it can create hindrances in situations where the data needs to be processed urgently. Additionally, it can also result in consent fatigue for organizations and information providers. Globally recognised data protection regimes such as the GDPR do not call for prior consent before undertaking transfer of PI. Obtaining valid, meaningful, and informed consent

of information providers for every processing activity is technically onerous, and likely to impair the user interface and experience, without enhancing data protection outcomes.

For the purposes of seeking access to data, government agencies should focus their investigation powers on entities that have access to and control over the data i.e. information/data regulators, and not data processors. Other jurisdictions also limit their requests for lawful access to data to entities responsible for generating such content (such as telecom operators and carriage service providers). Data processors, including hyperscale cloud service providers, would not be best placed to offer meaningful assistance to government agencies due to technical and practical limitations.

We therefore recommend that- (i) Rule 21 should be revised to remove consent as a prerequisite for transfer of PI, and (ii) Rules providing government agencies with the power to seek access to data should focus on data regulators, and not data processors; such rules are more appropriate for cybercrime laws, and not data protection laws.

z. **Storage Limitation**, *Rules 22 and 23*

These provisions imposes purpose limitation and storage/retention limitation restrictions on entities that collect data. The data needs to be destroyed after the purpose for which it was collected is achieved. However, these provisions will not apply in case of- (a) prior consent provided by a person for use of her information, and (b) for historical, statistical or research work.

Storage limitation requirement under the Rules do not provide sufficient flexibility, creates uncertainty, and may impede beneficial data processing. This may prevent businesses from improving their services by processing data, as it will prevent them from retaining personal data after the purpose of collecting the data is achieved.

Additionally, many of these requirements are also repeated under rule 11 of the Rules which obligates the information regulator to delete personal information under certain circumstances including withdrawal of consent, orders of a Court, illegality of the information amongst others.

We recommend that- (i) Personal information collected and processed for contractual necessity or legitimate business interests should be exempted from the application of rules 22 and 23, and (ii) Rule 11 can be merged with rules 22 and 23.

aa. **'Miscellaneous' provisions - Information gathering powers**, *Rule 38*

Information regulators and processors must provide any information requested by the Agency to the body corporate / company. The draft Privacy Rules do not provide exemptions from this broad obligation, nor do they limit the permissible uses of that information once received by the Agency or otherwise provide any safeguards to ensure that data collected by the Agency under this provision is necessary and proportionate to the purpose for which it is being sought. In the absence of any clear guidelines or safeguards on the implementation of this provision, there is ample scope for misuse, which could have adverse effect on a data regulators' and/or content creators' proprietary rights and legal obligations under the laws of other jurisdictions. Information gathering powers of this kind also create significant conflict of laws issues. For example, US companies are prohibited from complying with any data requests from Bangladeshi law enforcement, unless a U.S. court issued an order in response to a letter rogatory. In the interest of a predictable regime of law enforcement access to data, we recommend reformulating these provisions to address conflict of laws issues and to provide a rights-respecting

framework for surveillance requests which draws upon international human rights norms, and make up the bones of "lawfulness, legitimacy, necessity, and proportionality. For example:

- Lawful: Surveillance is established in law, and the crimes or activities investigated must adhere to established international human rights standards;
- Specificity: The data sought be bounded by a named/identified target and subject matter
- Independent Authorization: Demands for data are authorized or subject to review by a judicial or independent oversight body established under these rules
- Clarity of process: The process by which law enforcement/government officials may request data, for what purposes, how those data may be used, the scope of requests, etc. must be clear in law or regulation
- Data Protection: There must be clear rules or processes for protecting the privacy and data security of data subjects, and for minimizing the collection, retention, and use of data that is not relevant to the investigation
- Limited timeframe: Data requests must be for a specific period of time
- Oversight, transparency and notification: A government entity making a data request must be subject to robust independent oversight; must provide transparency about the nature, scope, scale, and authorizing authorities for its requests; and provide notice to and/or allow providers to notify data subjects when their data has been produced (subject to reasonable notification delays if notification would put a person in danger or would jeopardize an investigation)
- Redress: Providers and data subjects must have an opportunity to appeal or challenge a data request, and obtain redress if data is wrongfully demanded or used

We re-iterate our concerns, as given in the suggestions/ recommendations for rule 21 i.e. data processors should be kept outside the scope of provisions empowering the government to seek data from other companies. Such powers should be directed only at data regulators, as data processors do not exercise any kind of control over data. They cannot provide the government or its agencies access to data due to technical and practical limitations.

bb. **'Miscellaneous' provisions - No action where authorities have acted in 'good faith'**, *Rule 39*

Rule 39 of the draft Privacy Rules prevents legal action being taken against the GoB, the Director General of the Agency or any other person appointed by the Agency in relation to any action or process initiated under the Privacy Rules in good faith. However, an assessment of whether an action was taken in good faith is inherently subjective and fact-dependent, and can be undertaken by commencing legal proceedings. In any event, this provision cannot prevent any person aggrieved from commencing judicial review proceedings under Article 102 of the Constitution, making the provision redundant. We recommend deleting this provision in its entirety.

C. **Conclusion**

While the aim of the draft Privacy Rules is commendable, there are several provisions which would benefit from additional precision through amendments. Any regulatory intervention that is too onerous, or wordings that are inarticulate, or legislation incompatible with internationally accepted standards in a global ecosystem, would impede the role of online service providers in assisting communications and connectivity, driving commerce and knowledge-building, and sustaining innovation and governance. Consistent with the constitutional principles of Bangladesh, and with the objective to allow harmonious integration of the digital economy of Bangladesh with the rest of the world's, the suggestions and recommendations above were provided to assist the effort of the GoB to counterbalance the global best practices and address the specific concerns relating to Bangladesh.

Enclosure B

DETAILED COMMENTS AND RECOMMENDATIONS ON THE DIGITAL SECURITY AGENCY RULES, 2020

A. General Comments

The recently enacted Digital Security Rules, 2020 (**'DSA Rules/The Rules'**) are a notable effort by the Government of Bangladesh to provide clarity on the powers, duties, and responsibilities of key government authorities responsible for digital security in Bangladesh.

We appreciate the effort put into the DSA Rules by the Government of Bangladesh, especially with regards to clarifying the powers of the Digital Security Agency (the **'Agency'**), the Director General of the Agency (**'Director General'**), the National Computer Emergency Response Team (**'NCERT'**), and the Forensic Lab. However, we believe that the Rules, as implemented, serve as a missed opportunity to clarify the vague provisions present in the Digital Security Act, 2018 (the **'Act'**). Furthermore, neither were any due process safeguards integrated into the Rules that would bring the provisions of the Act, concerning the regulation of online content, in line with international human rights standards and the Constitution of Bangladesh. Such omissions are unfortunate given that the Constitution of Bangladesh states in Article 11 that fundamental human rights and freedoms are guaranteed.

We would therefore like to take this opportunity to give our comments and observations on the DSA Rules, and hope that the Government of Bangladesh would take these into consideration in revisiting the Rules with a view to strengthening Bangladesh's digital security regulation.

B. Content Regulation

Under Article 39 of the Constitution of Bangladesh, and Article 19 of the ICCPR (which Bangladesh is a party to), speech can only be restricted if necessary for the preservation of certain limited state interests (such as national security). Furthermore, any restriction on speech must be 'reasonable' under both Article 39 of the Constitution and Article 19 of the ICCPR, therefore making it mandatory for the principles of proportionality to be taken into consideration before any restriction on speech is imposed.

In addition to the protections afforded to free expression, the Constitution of Bangladesh also protects the right of individuals to due process and imposes an obligation on executive authorities to abide by the principles of natural justice. To fulfill the requirements of due process and natural justice, any order by an executive functionary has to contain adequate reasons for its decision.

The legal regime in Bangladesh therefore requires that every decision that has the consequence of restricting speech must be:

- In accordance with due process, i.e. based on fair, non-arbitrary, objective standards;
- In furtherance of one of the legitimate state interests given in Article 39 of the Constitution; and
- 'Reasonable' under the circumstances, i.e. proportionate to the aim sought to be achieved.

Unfortunately, neither the Act nor the Rules mandate that these factors be taken into consideration by law enforcement in making decisions concerning restricting or blocking speech online.

One instance of this is Section 8 (1) of the Act, which states that the Director General may request the Bangladesh Telecommunication Regulatory Commission (**'BTRC'**) to block or remove content that threatens digital security and falls within his jurisdiction. However, there are no due process or procedural safeguards in the Act or Rules that would serve as a check on this power. The Director General follows no objective standards in making its decision, and there is no protection against arbitrary decision-making. The Director General does not need to point out which legitimate state interest under Article 39 is being protected, and why the restriction is proportionate. These omissions ignore the important safeguards necessary to protect speech given in the Constitution of Bangladesh.

Similarly, Section 8 (2) grants law enforcement authorities the power to request BTRC to block or remove content if the content 'hampers the nation or any part therein in terms of nations unity, financial activities, security, defense, religious values, public discipline, or incites racism and hatred.' This section has the same problems as Section 8 (1) of the Act.

We believe that the Government of Bangladesh had the power to rectify these deficiencies by exercising the rule making power granted in Section 8 (4) and 60 (1) of the Act. However, the Rules do not make any reference to due process safeguards for the protection of free speech. We recommend that there should be express provisions incorporated into the Rules that provide due process protections limiting the powers of the Director General and law enforcement authorities to take down content. These safeguards should include:

- At a minimum, a *prima facie* assessment by the Director General or law enforcement authorities in writing that explains (i) which provision of law the offending content violates, and (ii) a written order with reasoning to support this decision backed by evidence.

- The reasoning given must be in line with the requirements of Article 39 of the Constitution and Article 19 of the ICCPR. This means that the following reasoning should support the decision to takedown content:

    a. Which legitimate state interest given in Article 39 is protected by the removal of the content.
    b. Why the removal of content is necessary and proportionate to the interest identified.

- Inclusion of a provision which would require a takedown request to be issued only where there is no alternative method or recourse available to remove access to the offending content (this would ensure taking into consideration the requirements of proportionality i.e. speech be restricted only when necessary); and

- Inclusion of a provision that states that every takedown request is to be accompanied by reasons supporting which legitimate state interest given in Article 39 of the Constitution is being invoked to block the content, and, why it has been found necessary to do so.

C. **Clarification on Powers and Responsibilities of Authorities**

The DSA Rules 2020 seemingly offer broad and overlapping powers to multiple authorities. The interplay of these powers is unclear. According to Rules 3 and 4 of the DSA Rules 2020, the powers, duties and functions of the Agency appear to be limited to coordinating and taking measures during a state crisis relating to the information technology, ensuring security of the critical information infrastructure, research and development, coordination amongst agencies, and undertaking necessary measures and investigation in relation to digital security. Similarly, the Director General has been conferred broad powers and duties under

Rule 5 of the DSA Rules 2020 which appears to be largely concentrated on security of critical information infrastructure, coordination activities, providing instructions and overseeing activities relating to digital security system, and taking action in relation to threat to information and communication technology. On the other hand, Rule 6 of the DSA Rules 2020 provides expansive powers to the NCERT to categorize, investigate and take all necessary measures to prevent digital attack, collection of information, forensic analysis and addressing deficiencies in digital security. While it is clear that the law enforcement and investigative functions are beyond the ambit of the powers of these authorities and are to be exercised by the law enforcement agencies under Section 39 of the DSA 2018, it appears that there are overlaps between the broad powers, duties and functions of the Agency, the Director General and the NCERT. We expect that the dichotomy of responsibilities and scope of these authorities would be further clarified by way of notification in official Gazette under Sections 59 or 60 of the Digital Security Act, 2018 ("**DSA 2018**"), or amendment to the DSA Rules 2020. We also expect that the powers of the National Security Council would be elaborated further, pursuant to Section 13(2)(e) of the DSA 2018.

D. Data Request Concerns

The provisions of the DSA Rules 2020 variously allow the Agency, the Director General and the NCERT to collect information relating to information and communication technology and digital security. However, the provisions are silent on the procedures under which these authorities may request information, the standards of security that the authorities will in practice have to maintain, and the period of retention. Further, the intended use of such information is not clear. We recommend that specific and express provisions should provide clear guidelines on these matters, by way of enactment of additional rules under Section 60 of the DSA 2018 or amendment and incorporation to the existing provisions of the DSA Rules 2020.

In addition, of particular concern is the provisions of Rule 7 of the DSA Rules 2020, which allows NCERT to request for information it deems relevant and all persons and entities have a positive obligation to comply with such requests. We would like to express our serious concerns in this regard as this provision is overly broad and without safeguards or oversight to ensure requests for information are specific and relevant to NCERT's purpose. Firstly, such requests do not appear to have any oversight, are not required to be backed by judicial order, and no procedures are prescribed to regulate NCERT's requests. Additionally, given the wording of the provisions, the mandatory compliance requirement raises stark privacy concerns for data regulators. Secondly, while Rule 7(4) of the DSA Rules 2020 allows the NCERT to ensure the confidentiality of the information collected and prevent its dissemination without prior permission of the data subject, this is contradicted by Rules 7(5) and Rule 10:

(i) under Rule 7(5) of the DSA Rules 2020, the NCERT can publish the information collected if it is in the interest of protecting digital security or creating awareness; and

(ii) under Rule 10 of the DSA Rules 2020, the NCERT can exchange any information relating to digital security with certain entities, including, for instance, relevant establishments providing digital security, telecommunication services, ICT services, research and development activities, as well as law enforcement agencies, both without prior permission of the data subject. In particular, Rule 10 of the DSA Rules 2020 allows wide powers to the NCERT to disseminate information to third parties without any security accreditation or confidentiality obligations, which is problematic from a security and privacy perspective.

Third, we understand that the DSA 2018 and, by extension the DSA Rules 2020, has extra-territorial applicability and this creates an untenable compliance issue for offshore entities providing services in multiple jurisdictions and who are subject to the data privacy and security laws of such jurisdictions. This is

particularly problematic with jurisdictions that may not allow such unregulated disclosure, especially in the absence of security standards required to be maintained by third party entities and where there are appreciable risks of disclosure without prior notice to the data subject. This provision also appears to be non-compliant with the draft of the Information Privacy and Security Rules, 2019 and against the spirit and letters of the Article 43 of the Constitution which guarantees the right of every citizen of Bangladesh to the privacy of his correspondence and other means of communication, and impedes upon the fundamental rights of every citizen to carry out any trade or business under Article 40 of the Constitution. Given that these interests are ensured under the Constitution, it is the duty of the GoB to adopt an approach to regulation which balances and seeks to harmoniously construe and apply the in practice.

E. **Digital Forensic Lab**

Under Rule 13 of the DSA Rules 2020, the Digital Forensic Lab has been established. The function of the Digital Forensic Lab is to analyze and provide expert opinion on digital evidence, and the technical and procedural specification thereof is provided in the Schedule to the DSA Rules 2020. However, the provisions of the DSA Rules 2020 are silent on the powers of the Digital Forensic Lab. Further, the term "digital evidence" is not defined in the DSA 2018 or the DSA Rules 2020. Additionally, it is unclear from the provisions as to the chain of order with respect to the operation of the Digital Forensic Lab. We would recommend clarifying these concerns, by amendment and incorporation to the existing provisions of the DSA Rules 2020.

F. **Conclusion**

In conclusion, we believe that the provisions indicated above would benefit from additional comprehensibility through amendments and further legislative activism under Section 60 of the DSA 2018. Any regulatory intervention that is too onerous or wordings that are inarticulate would make the provisions of the DSA Rules 2020 vulnerable to challenge in a court of law for want of constitutionality, under Article 102 of the Constitution. We recommend that the concerns highlighted above should be addressed and the relevant provisions should be brought in line with global standards, recommended practices and principles enshrined in the Constitution.