October 26, 2023

Anisul Huq MP
Minister, Ministry of Law, Justice and Parliamentary Affairs
Government of People's Republic of Bangladesh

Zunaid Ahmed Palak MP
Minister of State, Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
Government of People's Republic of Bangladesh

SUBMISSION ON THE DRAFT DATA PROTECTION ACT, 2023

Minister Huq and Minister Palak,

We welcome the opportunity to provide this submission on the latest draft of the *Data Protection Act, 2023* (the "Act"). We commend the initiative of the Information and Communication Technology Division to draft this important legislation to safeguard the privacy of individuals, aligned with the constitutional protections and obligations under the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Tech Global Institute is a global policy lab with a mission to reduce equity and accountability gaps between the internet ecosystem and the Global South. Access Now is an international non-profit organization which works to defend and extend the digital rights of users at risk globally. Our shared vision in making this submission is to ensure a well-balanced, future-proof, and rights-respecting framework aligned with international standards.

Please find our detailed submission and recommendations on the Act below.

1. ***Overly broad definitions to create compliance and enforcement challenges. Data protection laws are primarily designed to safeguard an individual's privacy rights in relation to their personal data; not all classes of data and all data owners entail the same level of risks or require the same level of protection.*** According to the title, preamble and application section of the Act, the legislation aims to protect *data of any person* — i.e., any information, knowledge, facts, ideas or opinions related to natural and non-natural persons. While the inclusive definitions reflect a well-intentioned desire for comprehensive protection, in reality, extending the application of the law to a broad spectrum of information and to juridical persons will be inconsistent with comparable data protection legislations worldwide and could also result in significant compliance and enforcement complexities. The conflation of individuals' personal information with other types of data, and common compliance and enforcement mechanisms, would lead to inadequate protection of the right to privacy.

We recommend amending the Act to replace all references to "data" with "personal data" so that only information relating to an identified or identifiable natural person is subject to statutory

protection, and protection measures must accordingly be amended to align with strict standards of necessity and proportionality. Clarification should be provided that an identifiable natural person is one who can be identified, directly or indirectly, with reference to identifiers, such as name, identification documents, location data, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity, trait, attribute or feature of that natural person, as well as technical, inferred or system-generated information about the natural person, such as geolocation data, internet protocol addresses, payment card information, online behavior, credit score, and employment history), whether online or offline, and shall include any data capable of being re-identified after undergoing a process of de-identification. In this context, "de-identification" means a process, informed by available best practices, applied to personal data that involves treating it in such a way such that the data subject is identified or reasonably identifiable. This will ensure that protection is commensurate with and proportionate to the sensitivity of the data.

2. ***Overly broad application to create enforcement and compliance challenges.*** According to section 4, the statute applies to the collection, processing, use, transmission and retention of *any data within and outside Bangladesh*. While in theory, extraterritoriality is necessary in this era of globalization and cross-border trade, the provision should be balanced and proportionate to avoid inordinately wide application. It extends the application of the law to non-resident entities and individuals if data is processed in relation to commercial activities or the profiling of *any data subjects*, irrespective of their nationality or location. This would likely result in jurisdictional disputes, deter new businesses from entering the market and is inconsistent with international best practices on human rights and privacy.

We recommend amending paragraph (c) of section 4(1) to limit the application of the law to the offshore processing of personal data, or profiling, of a data subject *resident in* Bangladesh. We draw your attention to the recently enacted Indian *Digital Personal Data Protection Act, 2023* ("Indian DPDPA") which apply to the processing of personal data 'outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.' Similarly, the Sri Lankan *Personal Data Protection Act, No. 9 of 2022* also applies to offshore processing where the firm 'offers goods or services to data subjects in Sri Lanka including the offering of goods or services with specific targeting of data subjects in Sri Lanka' or 'specifically monitors the behaviour of data subjects in Sri Lanka including profiling with the intention of making decisions in relation to the behavior of such data subjects in so far as such behaviour takes place in Sri Lanka.' Furthermore, the EU's *General Data Protection Regulation* ("EU GDPR") applies to the processing of personal data by non-resident establishments only if the data subject is in the EU and 'the processing activities are related to the offering of goods or services … to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within [EU].'

3. ***Over-reliance on a rule-based system creates unaccountability and unpredictability, as well as compliance and enforcement challenges.*** Delegation of the rule-making and direction-issuing authorities to the executive branch under sections 40, 42, 45, 65, 68 and 70 encroaches upon principles of separation of powers and parliamentary democracy and is inconsistent with best practices on data protection legislations worldwide. We note that such delegation blurs the distinct roles and lines of accountability among different branches of government, inculcates a democratic deficit in the legislative

process, inhibits parliamentary scrutiny, creates opportunities for regulatory capture, and contributes to an undue concentration of power within the executive branch. It raises substantive gaps in how the Act should be enforced and complied with, confers expansive powers on the rule-making authority, that would adversely impact people's rights, as well as predictability of the regime which is crucial for legitimate business interests. Absent robust mechanisms to ensure proportionality, transparency and accountability in the exercise of these delegated authority, there are risks of abuse of the mandate.

We recommend amending the Act to limit over-reliance on delegated rule-making authority and secondary legislations, instead articulating substantive provisions in sufficient detail in the Act to establish clear and published standards to regulate conduct, fostering transparency and accountability in the legal framework, reduce regulatory overhead, and provide a smoother transition to the implementation of the Act.

We further recommend that, in the interest of a predictable regime that supports collaborative rule-making approach, the Act should incorporate an express provision reiterating its obligations under the *Rules of Business* to have the rules pre-published in an official gazette and on its website soliciting input from the relevant stakeholders, before it is enacted using an executive order.

4. ***Discretion to define "classified data" risks inconsistent interpretation and application.*** While mandating localization of classified data, the statute falls short of explaining the term and instead empowers the executive branch of the government to prescribe definition via secondary legislations. Granting non-legislative authority broad discretion to define critical terms in a statute and shape the law's interpretation can be problematic, as addressed above. If the discretion is not exercised with caution, it could result in an overly broad definition, thereby enabling localization and restrictions on cross-border transfer of data designated as such, and an enhanced scope for opaque surveillance. A well-drafted statute should aim to provide clear and unambiguous language to guide its implementation.

We recommend amending the Act to clearly and exhaustively define "classified data" that establishes clear and published standards for localization and cross-border transfer restrictions. It should not delegate authority to the executive branch to alter or expand the definition.

5. ***Discretion to access data without procedural safeguards risks violating the rights of the data subject.*** According to section 10(2)(d) of the Act, any data may be collected from a data subject if it is deemed necessary for national security or prevention or detection of an offense. It neither specifies well-defined conditions nor any third party or judicial oversight in the event data needs to be collected for an investigation. The provision also introduces inconsistencies with data access provisions of the Cyber Security Act, 2023, the Bangladesh Telecommunications Regulatory Act, 2001, and similar legislations that would result in compliance and enforcement challenges. We are concerned that the provision poses high risks of privacy and human rights abuse and mishandling by the data collector, which remains unspecified in section 10(1). We draw your attention to the observation by the High Court Division of the Supreme Court of Bangladesh in *The State vs. Oli* [2019] that accessing customer data by government agencies without following due process or informing the users constitute violation of the right to privacy guaranteed under Article 43 of the Constitution of Bangladesh.

We recommend amending section 10 to limit collection and access of data from a data subject to clearly defined necessary, proportionate and legitimate purposes with independent judicial oversight. Any request to collect data should be accompanied by procedural safeguards and limitations on what specific data can be collected, for how long, its use and disclosure to other parties, its retention and deletion standards and the rights of the data subject under the law to ensure data access does not encroach on their individual privacy.

6. ***Wide scope of exemptions and discretionary powers to undermine privacy protections and do not comply with the principles of necessity and proportionality.*** Some of the exemptions in the draft, such as the exemption for processing regarding "journalistic, literary, artistic or academic subjects" are well-intentioned and welcome. However, the exemptions for the purpose of preventing crime or levying taxes or duties are too broad and lack specificity, which could undermine individual privacy. Similarly, the exemption for processing health data could also undermine privacy as health data is sensitive personal information. Each exemption needs to be strictly qualified and its rationale grounded in privacy principles. It is also not clear which provisions of the law will be applicable and which will be not applicable, as this appears to have been left to the government to decide. Furthermore, the unfettered mandate to give further exemptions in section 34, without any qualification, is susceptible to misuse. We note that these exemptions are in addition to the broad grounds for processing without consent permitted under section 7, which specifically allows in sub-section (6) processing for "any matter relating to public interest" — an allowance that is inherently vague, left to delegation in the rules, and could be interpreted broadly.

We recommend deleting sections 34 and 7(6) in its entirety as there should be no provision enabling the government to grant unqualified and unchecked exemptions to the Act. We further recommend amendment to sections 33 and 7(5) to restrict the scope for misuse of the exemptions and remove avoidable ambiguities in the application of the law. The legislation should clearly state the sections whose application may be exempted for relevant reasons, and incorporate safeguards aligned with the principles of necessity and proportionality, to protect people's data and privacy.

7. ***Lack of independence of the proposed Data Protection Board and the appellate authority leaves individuals without fair and meaningful judicial remedy.*** Control over the Data Protection Board and the appellate authority is vested with the government, with the government having the absolute mandate to appoint its members, determine the terms and conditions of their service, and lay down policies that must be complied with while carrying out their functions. An independent regulatory or oversight authority is essential for ensuring protection of individual rights, particularly because the government and its agencies and instrumentalities are likely to be large data fiduciaries under the law. Aggrieved persons and entities must have the right to approach an independent adjudicatory authority with complaints and appeals to seek remedy.

We recommend amending Chapters IX and XIII to ensure that the Data Protection Board and the appellate authority is completely independent from the government and its agencies, including in its composition, appointments, formulation of policies and guidelines, procedures and functioning.

While the Data Protection Board may cooperate and coordinate action with other government agencies and independent regulatory authorities once established, their powers, functions and responsibilities should not be conflated. Furthermore, the appellate authority must be independent, either constituted as a quasi-judicial body composed of retired judges of the High Court Division of the Supreme Court of Bangladesh and legal experts, or constituted as a judicial body. We note that earlier consultation drafts contained tiered appellate procedure that allowed aggrieved persons to approach the cyber tribunals and cyber appellate tribunals established under the the Information and Communication Technology Act, 2006, which has been omitted from the current draft. We recommend reinstatement of those provisions, as otherwise every decision of the appellate authority will likely be challenged under the writ jurisdiction of the Supreme Court of Bangladesh.

8. ***Absence of the right of individuals to be informed about data breaches undermines the right to privacy.*** Affected individuals must be informed of any data breach in recognition of their ownership of their own personal data, autonomy to control their personal information and make informed choices about its use, their right to privacy, and their right to claim compensation. When individuals are not promptly informed of data breaches, their ability to take necessary precautions, such as changing passwords, monitoring financial accounts, or protecting themselves from identity theft, is severely compromised, leaving individuals exposed to the often detrimental consequences of data breaches.

We recommend amending section 28 to mandate that all affected individuals be notified of the breach of security of their data, with clear articulation of available remedies, within seventy-two hours (i.e., the same timeframe as has been prescribed for the Data Protection Board).

9. ***Lack of a well-scoped definition of "erasure right" risks inconsistent interpretation and misuse.*** The right to erasure is important for data subjects. However, while well-intentioned, this provision, in its current form, empowers individuals to request companies to *erase* extensive volumes of data about them based on broad grounds like irrelevance and objections to data processing. Although designed to grant individuals control over their personal data, without a clear definition and limitations, this provision would allow governments and data-fiduciaries to interpret and apply it in a manner that serves their own interests rather than those of data subjects, raising concerns about new avenues for unwarranted content restriction. Conventional rules of statutory interpretation mandate that words be understood in their plain and grammatical sense (with certain exceptions), and, therefore, a literal interpretation could interpret this right as necessitating the complete removal of content, even when its accuracy or legitimacy is undisputed, leading to censorship and informational obscurity. Given the law's extraterritorial reach, an erasure order might trigger global enforcement obligations. On the other hand, a more lenient reading of the term permits data-fiduciaries to merely obscure, geo-block, or archive information rather than entirely eliminating it from their systems as an effective form of redress for data subjects in certain circumstances. The right to erasure must be balanced with the right to free expression and right to information. The law must clearly spell out the factors to be considered, and the limitations and legal principles to be followed, including necessity and proportionality, to facilitate effective and predictable implementation. Given that enforcement of the right can be exempt when weighed against freedom of expression or the public interest, each of which is subject to varying interpretations and inconsistent applications, clear and unambiguous definitions and safeguards are imperative. In the

absence of such clarity and rights-respecting safeguards, the underlying uncertainties would be prone to misuse, and selective application by those in power, rendering data subjects' rights meaningless in practice.

We recommend incorporating clear definitions and safeguards in respect of the right to erasure in section 18 and elsewhere in the Act in unambiguous terms, in order to ensure consistent interpretation and application of the right and to avoid misuse both by the state agencies and data-fiduciaries, and prioritization of the rights of data subjects.

10. ***Lack of proportionate penalties for violations to result in uneven application and outcomes.*** Prescribing maximum fine amounts without regard to the size of the data fiduciary could lead to difficulties in imposing the administrative fines and result in relatively low fines being imposed on large data fiduciaries profiting from unlawful personal data processing activities. Administrative fines imposed in each individual case should be effective, proportionate and dissuasive, based on consideration of the overall circumstances of the infringement. Assessment should include the nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, actions taken (including technical and organizational measures) to mitigate the risk of infringement, repetitive nature of the infringement, previous non-compliances, categories of personal data affected, and other aggravating or mitigating factors, such as financial benefits gained or losses avoided from the infringement. Notably, laws in other jurisdictions have a much higher threshold and multifaceted criteria for fines. For instance, the EU GDPR prescribes maximum fine of the higher of € 20 million or 4% of the worldwide annual turnover in the preceding financial year (decreasing to € 10 million or 2% of the turnover for less serious infringements), while the penalties under the Indian DPDPA generally ranges between ₹ 500 million to ₹ 2.5 billion (with ₹ 10,000 as the lowest amount of fine for lesser infractions). Under the proposed framework in Bangladesh, the maximum fine amount ranges between BDT 200,000 and 500,000 (~ US$ 1,800 to 4,500).

We recommend amending Chapter XII to set a higher threshold of at least BDT 100 million (~ US$ 900,000), requiring the authority to consider the overall circumstances of the infringement (including each of the factors outlined above) and the average worldwide turnover for the last three preceding financial years, provided that the fine should not be more than ten percent of such amount. Fines imposed must be demonstrably effective, proportionate and dissuasive relative to the infringement.

11. ***Lack of proper purpose and time limitations on retention of data does not comply with the principle of data minimization.*** Data minimization is a core tenet of privacy and data protection laws, emphasizing that organizations should only collect, process, and retain personal data to the extent necessary to achieve a specific, legitimate purpose. In the absence of clear legislative provisions specifying the purpose and duration for which data can be retained, there is a heightened risk of unnecessary and excessive data storage, which not only poses privacy concerns but also increases the likelihood of misuse or data breaches. By incorporating explicit purpose and time limitations within the legal framework, the legislation serves as a critical safeguard, aligning data management practices with the core principles of data protection, and ultimately contributing to a more responsible and rights-

respecting data ecosystem. The legislation must clearly prevent retention of data after it has fulfilled its legitimate purpose, rather than leaving this important principle to be addressed in the rules, as that may result in inconsistency, lack of enforcement, and potential misuse of personal data.

We recommend amending section 25(1) and other provisions on retention of data to categorically adhere with principles of data minimization, purpose limitation, necessity and proportionality.

We thank the Government of Bangladesh for the opportunity to share our views on the Data Protection Act, 2023. We are happy to provide clarification on any aspect of our submission, or to offer inputs and insights directly through meetings and official consultations.

Should you have any questions or need clarification, please do not hesitate to contact us.

Thank you again for your time and consideration.

Sincerely,

Access Now
Tech Global Institute