Jurisdiction	Bangladesh
Date	March 26, 2022
Law Firm	Doulah & Doulah
Title, Name	A.B.M. Nasirud Doulah, Partner
Contact Information	ndoulah@doulah.net, +8801711506015

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the private sector at the present or in the near future?

Bangladesh has a general law (Bangladesh Digital Security Act, 2018) which covers protection of personal information. There is also another law (Bangladesh Information & Communication Technology Act, 2006) that deals with unauthorized access of data. In addition, it is also planning to introduce a dedicated privacy act.

ii. Does your country have a general law concerning protection of personal information in the public sector at the present or in the near future?

The same laws as stated above are applicable to public sector.

iii. Does your country have laws concerning protection of personal information which apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.)

There are also some industry specific laws that covers protection of personal information to some extent as described below:

- Bangladesh Telecommunication Act, 2001: Prohibits disclosure of subscriber meta data and provides and prohibits for interception of calls except by law enforcing agencies.
- Guideline on ICT Security for Scheduled Banks and Financial Institutions ('the ICT Guideline') imposes certain measures to secure all data and information used in the banking sector including personal data handling and cybersecurity related measures. Such measures include encryption, disaster recovery, security process.

- The National Blockchain Policy of Bangladesh, issued in March 2020, re-emphasises cybersecurity measures in line with the Digital Security Act while confirming the feasibility of any blockchain-based platform or transaction.
- Registered practitioners of the Bangladesh Medical & Dental Council ('BMDC') are subject to professional confidentiality agreements established with patients under the Code of Medical Ethics. Moreover, the BMDC Telemedicine Guidelines require the implementation of adequate cybersecurity measures for the participating institutions.
- Digital Commerce Operational Guideline 2021 covers different aspects of data protection on technological platforms such as consent requirements for cookies etc.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I.. (please add a reply column as necessary,)

The title of the law ：(Bangladesh Information & Communication Technology Act, 2006 (Technology Act)

① The definition of "Personal Information"	No express definition provided
② The scope in which the law applies	This law prohibits unauthorized access of any data in any system without the consent of the data owner. Whoever commits the offence of disclosing confidential and private information shall be punishable with imprisonment for a term that may extend to two years, and/or with a fine which may extend to BDT 200,000.
③ The territorial scope	Following are the territorial scope for this law: • if any person commits an offence or contravention outside of Bangladesh which is punishable under these provisions, then this Act shall apply as if they had committed such offence or contravention in Bangladesh; • if any person commits an offence or contravention in Bangladesh under these provisions from outside Bangladesh using a computer, computer system, or computer network located in Bangladesh, then these provisions shall apply as if the entirety of the offence or contravention took place in Bangladesh; and

	• if any person from within Bangladesh commits offence or contravention outside of Bangladesh under these provisions, then these provisions shall apply against them as if the entire process of the offence or contravention took place in Bangladesh.

The title of the law ： Bangladesh Digital Security Act, 2018 (Digital Security Act)

① The definition of “Personal Information”	Personal data is not expressly defined. However, the Digital Security Act expressly defines 'identity information' as any information which is biological or physical or any other information which uniquely or jointly with other information can identify a person (which includes body corporates) or system, whose name, photograph, address, date of birth, mother's name, father's name, signature, national identification card, birth and death registration number, finger print, passport number, bank account number, driving licence, E-TIN number (i.e. electronic tax identification number), electronic or digital signature, user name, credit or debit card number, voice print, retina image, iris image, DNA profile, security related personal data, or any other identification which, due to the facilitation of technology, is easily available.
② The scope in which the law applies	If any person without any legal authority collects, sells, takes possession, supplies or uses any person's identity information, then this activity will be an offence under the Act. If any person commits any such offence, the person may be punished with imprisonment for a term not exceeding five years and/or a fine not exceeding BDT 500,000 (approx. €4,970). In addition, this law prohibits unauthorized access of any data in any system without the consent of the data owner.
③ The territorial scope	Following are the territorial scope for this law: • if any person commits an offence or contravention outside of Bangladesh which is punishable under these provisions, then this Act shall apply as if they had committed such offence or contravention in Bangladesh; • if any person commits an offence or contravention in Bangladesh under these provisions from outside Bangladesh using a computer, computer system, or computer network located in Bangladesh, then these provisions shall apply as if the entirety of the offence or contravention took place in Bangladesh; and • if any person from within Bangladesh commits offence or contravention outside of Bangladesh

	under these provisions, then these provisions shall apply against them as if the entire process of the offence or contravention took place in Bangladesh.

ii. If there are any special instructions about the laws, please describe them.

These have been addressed above.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

These provisions have not been expressly adopted. However, the above said legislations address some of these principles as stated below:

(a) Collection Limitation Principle

As per Digital Security Act, if any person without any legal authority collects, sells, takes possession, supplies, or uses any person's identity information, then that activity will be an offence under the Act.

The data subject may give his/her prior specific informative consent for processing or relevant purpose irrespective of any consideration. In addition to prior specific informative consent, consent may also be granted on terms inserted in the related contract for the subject matter. The person may supply data on their own with some pre-determined usage granted. In order the to get the consent from the data subject, as stated above, the data controller can either grant prior specific informative consent or such consent may also be granted on terms inserted in the related contract for the subject matter. In addition to consent, the data controller can also process data to which they are contractually or statutorily authorized to process without any additional consent.

(b) Data Quality Principle

There is no provision relating to this.

(c) Purpose Specification Principle

(d) Use Limitation Principle

The data subject may give his/her prior specific informative consent for processing or relevant purpose irrespective of any consideration. In addition to prior specific informative consent, consent may also be granted on terms inserted in the related contract for the subject matter. The person may supply data on their own with some pre-determined usage granted. In order the to get the consent from the data subject, as stated above, the data controller can either grant prior specific informative consent or such consent may also be granted on terms inserted in the related contract for the subject matter. In addition to consent, the data controller can also process data to which they are contractually or statutorily authorized to process without any additional consent. Use is limited to the extent consent has been accorded for. Access and use of data belonging to a data user on the grounds of public interest is only allowed by law enforcement agencies per the Digital Security Agency.

(e) Security Safeguards Principle

Not addressed.

(f) Openness Principle

Not addressed.

(g) Individual Participation Principle

Not addressed.

(h) Accountability Principle

There is no provision on accountability principle. As per Section 52 of the Consumers' Rights Protection Act, 2009, whoever, in violation of any prohibition under any law for the time being in force, does any act which is detrimental to a service receiver's life or security, shall be punishable to imprisonment for a period not exceeding three years and/or a fine not exceeding BDT 200,000 (approx. €1,980). Under Section 53, any service provider who by its negligence,

irresponsibility, or carelessness damages the service receiver's finances or health, or causes death, shall be punishable to imprisonment for a period not exceeding three years and/or a fine not exceeding BDT 200,000 (approx. €1,980). In addition, the consumer may be entitled to claim damages.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

OECD Privacy Principle has not been expressly adopted and there is no sector in which any laws exclude the application of each OECD Privacy Principle.

(a) Collection Limitation Principle

(b) Data Quality Principle

(c) Purpose Specification Principle

(d) Use Limitation Principle

(e) Security Safeguards Principle

(f) Openness Principle

(g) Individual Participation Principle

(h) Accountability Principle

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as comprehensive government access to personal data or Data Localization? If yes, please describe them.

Under current framework there is no data localization requirements except for telecom sector where localization or certain aggregation points are mandatory.

Technology Act:

Pursuant to the Technology Act, the Government of Bangladesh ('the Government') has the power to intercept data provided that certain conditions are fulfilled. In particular, Section 46 of the Technology Act, which is an exception to the general rule for maintenance of privacy and secrecy of information, provides that the Government may intercept data where it is satisfied that such interception is necessary in the interest of:

- the sovereignty, integrity, or security of the state;
- friendly relations with foreign states;
- public order;
- for preventing incitement to the commission of any cognisable offence relating to the above; or
- for investigation of any offence.

The Government may, by order, direct any agency of the appropriate government authority to intercept, monitor or decrypt, or cause to be intercepted, monitored, or decrypted, any information generated, transmitted, received, or stored in any computer resource. Section 46 of the Technology Act empowers the Government to intercept, monitor, or decrypt any information, including information of a personal nature in any computer resource. Where the information is such that it ought to be divulged in the public interest, the Government may require disclosure of such information. Information relating to anti-national activities which are against national security, breaches of the law or statutory duty or fraud may come under this category.

Under the above circumstances, the controller, appointed by the Government, can direct a subscriber to extend facilities to decrypt, intercept, and monitor information. The scope of Section 69 of the Technology Act includes both interception and monitoring along with decryption for the purpose of investigating cybercrimes. The controller may, by notification in the Bangladesh Government Press or in the electronic gazette, declare any computer, computer system, or computer network to be a protected system and authorise applicable persons to secure access to protected systems.

The Digital Security Act

Under the Digital Security Act, if any data or information published or propagated in digital media regarding a subject that comes under the purview of the Director General which threatens data security, then the Director General can request the relevant regulatory authority to remove or block said data or information as appropriate.

Telecommunication Act

Under section 97(Ka) of the Telecommunication Act, 2001 (BTA) on the grounds of national security and public order, the government may empower certain government authorities (intelligence agencies, national security agencies, investigation agencies, or any officer of any law enforcement agency) to suspend or prohibit the transmission of any data or any voice call, and record or collect user information relating to any subscriber to a telecommunications service. This widely drafted provision encompasses interception capabilities. The relevant telecoms operator must provide full support to the empowered authority to use such powers. The BTRA (Bangladesh Telecom Regulatory Commission) does not provide for any time limits on these powers. As a result, an interception may last for as long as the agency implementing the interception decides.

Under the broad powers granted in section 97(Ka) on the grounds of national security and public order, the government may require a telecommunications operator to keep records relating to the communications of a specific user. However, when considering whether to give a retention request, the relevant government agency would need to consider the technical resources and capabilities of the operator to retain information.

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

Under the Digital Security Act the National Digital Security Council has been entrusted with the authority that can formulate and issue data protection guidance as and when required. However, for executive matters such as blocking a content or decrypt a data source, the Digital Security Agency has the executive power. However, these are the

administrative authorities for broad policy and internal control matters. In general the usual law enforcing agencies are the authorities that are entrusted to oversee operational aspects of the subject matter.