

地域	バングラデシュ人民共和国
日付	2022年3月26日
法律事務所	Doulah & Doulah
役職名、氏名	A.B.M. Nasirud Doulah, パートナー
連絡先	ndoulah@doulah.net , +8801711506015

質問事項

I. 個人情報保護に関する法律

- i. あなたの国には、現在又は近い将来施行される予定の私的分野における個人情報保護に関する一般法はありますか。

バングラデシュには、個人情報の保護を対象とした一般法(2018年バングラデシュ・デジタル・セキュリティ法)があります。また、データの不正アクセスに関する別の法律(2006年バングラデシュ情報通信技術法)もあります。さらに、専用のプライバシー法の導入も計画されています。

- ii. あなたの国には、現在又は近い将来施行される予定の公的分野における個人情報保護に関する一般法はありますか。

公的分野においても上記と同様の法律が適用されます。

- iii. あなたの国には、現在又は近い将来施行される予定の個別の(特定の)分野に適用のある個人情報保護に関する法律はありますか。(ある場合は概要を教えてください。)

また、以下のような、個人情報の保護についても一定程度カバーする業界特有の法律もあります。

- 2001年バングラデシュ電気通信法: 加入者のメタデータの開示を禁止し、通話傍受について定め、法執行機関以外の者による通話傍受を禁止しています。

- スケジュールドバンク及び金融機関のためのICTセキュリティに関するガイドライン(以下、「ICTガイドライン」といいます。)は、個人データの取扱いやサイバーセキュリティ関連の措置を含め、金融部門で使用されるすべてのデータや情報を保護するための一定の措置を課しています。そのような対策には、暗号化、災害復旧、セキュリティプロセスなどが含まれます。

- 2020年3月に発行されたバングラデシュの国家ブロックチェーンポリシーは、デジタルセキュリティ法に沿ったサイバーセキュリティ対策を再度強調する一方で、ブロックチェーンに基づくあらゆるプラットフォームや取引の実現可能性を確認しています。

- バングラデシュ医科歯科審議会(以下、「BMDC」といいます。)の登録開業医は、医療倫理綱領に基づき、患者との間で締結された職業上の秘密保持契約の対象となります。

さらに、BMDC 遠隔医療ガイドラインでは、関係者に適切なサイバーセキュリティ対策の実施を求めています。

- 2021 年デジタル・コマース運用ガイドラインは、クッキーの同意要件など、技術的なプラットフォームにおけるデータ保護のさまざまな側面をカバーしています。

I の(i)(ii)(iii)について全て「該当なし」の場合は IV に進みます。

II. 個人情報の保護に関する規程の基本情報

- i. I で言及いただいた個人情報保護に関する法律全てについて以下の空欄を埋めて下さい(必要に応じて回答欄を追加してください)。

名称: 2006 年バングラデシュ情報通信技術法 (技術法)

① 「個人情報」の定義	明確な定義はありません。
② 法律の適用範囲	この法律は、データ所有者の同意なく、システム内のデータに不正にアクセスすることを禁止しています。機密情報及び個人情報の開示という犯罪を行った者は、2 年以下の懲役及び/又は 20 万 BDT 以下の罰金に処されるものとされています。
③ 地理的範囲	この法律の地理的な適用範囲は以下のとおりです。 - 何人かがバングラデシュ国外でこれらの規定により処罰される犯罪又は違反を犯した場合、この法律は、その者がバングラデシュでかかる犯罪又は違反を犯したかのように適用されるものとします。 - 何人も、バングラデシュ国外からバングラデシュにあるコンピュータ、コンピュータシステム、又はコンピュータネットワークを使用して、バングラデシュにおいて、これらの規定のもとで犯罪又は違反を犯した場合、これらの規定は、犯罪又は違反の全体がバングラデシュで行われたかのように適用されます。 - バングラデシュ国内の者が本規定のもとで、バングラデシュ国外において犯罪又は違反を犯した場合、これらの規定は、犯罪又は違反の全過程がバングラデシュで行われたかのように、その者に対して適用されるものとします。

名称: 2018 年バングラデシュ・デジタル・セキュリティ法 (デジタル・セキュリティ法)

① 「個人情報」の定義	個人データは、明確に定義されていません。しかし、デジタル・セキュリティ法は「識別情報」を、生物学的又は物理的な情報、又は、単体若しくは他の情報と共同で個人(法人を含む。)やシステムを識別できるあらゆる情報である
-------------	---

	<p>り、名前、写真、住所、生年月日、母親の名前、父親の名前、署名、国民 ID カード、出生・死亡登録番号、指紋、パスポート番号、銀行口座番号、運転免許、E-TIN 番号(例えば、電子納税番号。)、電子署名又はデジタル署名、ユーザー名、クレジットカード又はデビットカード番号、声紋、網膜画像、虹彩画像、DNA プロファイル、セキュリティ関連の個人データ、又は技術の進歩により容易に入手可能となったその他の識別情報と定義しています。</p>
② 法律の適用範囲	<p>法的権限のない者が個人の識別情報を収集、販売、保有、提供、又は利用した場合、その行為は同法違反となります。このような犯罪を行った場合、その者は 5 年以下の懲役及び／又は 50 万 BDT(約 4,970 ユーロ)以下の罰金に処される可能性があります。</p> <p>さらに、この法律では、データ所有者の同意なしに、システム内のデータに不正にアクセスすることを禁止しています。</p>
③ 地理的範囲	<p>この法律の地理的な適用範囲は以下のとおりです。</p> <ul style="list-style-type: none"> - 何人かがバングラデシュ国外でこれらの規定により処罰される犯罪又は違反を犯した場合、この法律は、その者がバングラデシュでかかる犯罪又は違反を犯したかのように適用されるものとします。 - 何人も、バングラデシュ国外からバングラデシュにあるコンピュータ、コンピュータシステム、又はコンピュータネットワークを使用して、バングラデシュにおいて、これらの規定のもとで犯罪又は違反を犯した場合、これらの規定は、犯罪又は違反の全体がバングラデシュで行われたかのように適用されます。 - バングラデシュ国内の者が本規定のもとで、バングラデシュ国外において犯罪又は違反を犯した場合、これらの規定は、犯罪又は違反の全過程がバングラデシュで行われたかのように、その者に対して適用されるものとします。

- ii. 上記の法について特に言及すべき事項がございましたらその概要をご教示下さい。
上記のとおりです。

III. OECD プライバシーガイドライン

- i. OECD プライバシーガイドラインの各原則を体現した法の規定があればその概要をご教示下さい。
- <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandtransborderflowsofpersonaldata.htm>

これらの原則は、明示的に採用されているわけではありません。しかし、上記の法律では、以下に示すとおり、これらの原則のいくつかに対応しています。

(a) 収集制限の原則

デジタル・セキュリティ法によると、いかなる者も法的権限を持たずに個人の識別情報を収集、販売、保有、提供、又は利用した場合、その行為は同法違反となります。

データ主体は、対価の如何を問わず、処理又は関連する目的について事前に具体的な情報を得たうえで同意を与えることができます。事前の具体的な情報を得たうえでの同意に加え、対象に関連する契約に挿入された条件によって、同意を得ることもできます。人は、あらかじめ決められた使用方法に従って、自らデータを提供することができます。上記のようにデータ主体の同意を得るために、データ管理者は事前に具体的な情報を得たうえでの同意を認めるか、又は対象に関連する契約に挿入されている条件に基づいてそのような同意を認めることができます。同意に加えて、データ管理者は、契約上又は法令上処理することが認められているデータを、追加の同意なしに処理することができます。

(b) データ内容の原則

この原則に関する規定はありません。

(c) 目的明確化の原則

この原則に関する規定はありません。

(d) 利用制限の原則

データ主体は、対価の如何を問わず、処理又は関連する目的について事前に具体的な情報を得たうえで同意を与えることができます。事前の具体的な情報を得たうえでの同意に加え、対象に関連する契約に挿入された条件によって、同意を得ることもできます。個人は、あらかじめ決められた使用方法に従って、自らデータを提供することができます。上記のようにデータ主体の同意を得るために、データ管理者は事前に具体的な情報を得たうえでの同意を得るか、又は対象に関連する契約に挿入されている条件に基づいてそのような同意を得ることができます。同意に加えて、データ管理者は、契約上又は法令上処理することが認められているデータを、追加の同意なしに処理することができます。利用は、同意の範囲内のものに限定されます。公共の利益を理由とするデータ利用者のデータへのアクセス及び使用は、デジタル・セキュリティ・エージェンシーに従って法執行機関によってのみ許可され

ます。

(e) 安全保護の原則
対応していません。

(f) 公開の原則
対応していません。

(g) 個人参加の原則
対応していません。

(h) 責任の原則
責任の原則に関する規定はありません。2009年消費者権利保護法第52条によると、現行法に基づく禁止事項に違反し、サービスの提供を受ける者の生命又は安全を害する行為を行った者は、3年以下の懲役及び/又は20万BDT(約1,980ユーロ)以下の罰金に処されるものとされています。第53条では、サービス提供者が過失、無責任、不注意により、サービスの提供を受ける者の財産や健康に損害を与え、又は死亡させた場合、3年以下の懲役及び/又は20万BDT(約1,980ユーロ)以下の罰金に処されるものとされています。また、消費者は損害賠償を請求することができます。

ii. OECD プライバシーガイドラインの各原則が適用されない分野があればその概要を教えてください。

OECD のプライバシー原則は明示的に採択されておらず、OECD の各プライバシー原則の適用を排除する法律が存在する分野もありません。

(a) 収集制限の原則

(b) データ内容の原則

(c) 目的明確化の原則

(d) 利用制限の原則

(e) 安全保護の原則

(f) 公開の原則

(g) 個人参加の原則

(h) 責任の原則

IV. ガバメントアクセスとデータローカライゼーション

あなたの国において、包括的なガバメントアクセスやデータローカライゼーションのような、個人データの主体の権利に影響を及ぼすような仕組みはございますか。ある場合は、その内容をご教示下さい。

現在のフレームワークでは、ローカライゼーションまたは特定のアグリゲーションポイントが義務付けられている通信分野を除き、データローカライゼーションの要求はありません。

技術法

技術法により、バングラデシュ政府(以下「政府」といいます。)は、一定の条件が満たされることを条件に、データを傍受する権限を有しています。特に、技術法第 46 条は、プライバシー及び情報の秘密性の保持の一般規則の例外として、以下の利益のために傍受が必要であると認められる場合、政府がデータを傍受することができると規定しています。

- 国家の主権、領土保全、又は安全保障。
- 外国との友好関係
- 公の秩序
- 上記に関連する認知可能な犯罪遂行の扇動を防止するため
- 犯罪の捜査のため

政府は、命令により、適切な政府当局の機関に、コンピュータリソースで生成、送信、受信、又は保存された情報を傍受、監視、又は解読するよう指示し、又は傍受、監視、又は解読させることができます。また、技術法第 46 条は、あらゆるコンピュータリソース内の個人的な性質を持つ情報を含むあらゆる情報を傍受、監視、解読する権限を政府に与えています。情報が公共の利益のために開示されるべきものである場合、政府はその情報の開示を要求することができます。国家の安全保障違反、法律や法的義務違反、詐欺行為といった反国家的活動に関する情報は、このカテゴリーに含まれる場合があります。

上記の状況下において、政府によって任命された管理者は、情報の解読、傍受、及び監視のための設備を拡張するよう署名者に指示することができます。技術法第 69 条の範囲には、サイバー犯罪を捜査する目的の復号化に加え、傍受と監視の両方が含まれます。データ管理者は、バングラデシュ政府出版局による通知、又は電子官報での通知により、コンピュータ、コンピュータシステム、コンピュータネットワークが保護されたシステムであると宣言し、該当する人物に保護システムへのアクセスを認める権限を付与することができます。

デジタル・セキュリティ法

ディレクタージェネラルの管轄下にある対象に関し、データ又は情報がデジタルメディアで公開又は伝播され、データセキュリティを脅かす場合、デジタル・セキュリティ法に基づき、ディレクタージェネラルは関連する規制当局に当該データ又は情報の削除又はブロックを適宜要請することができます。

電気通信法

2001 年電気通信法(BTA)第 97 条(Ka)に基づき、国家の安全及び公の秩序を理由として、政府は特定の政府当局(情報機関、国家安全保障機関、捜査機関、法執行機関の役員)に対し、データ送信又は音声通話を停止又は禁止し、電気通信サービスの加入者に関するユーザー情報を記録又は収集できる権限を与えることができます。この広範な規定は、傍受できる権限を包含しています。関連する電気通信事業者は、権限を与えられた当局がこのような権限を行使する際に、全面的に協力しなければならないとされています。BTRA(バングラデシュ通信規制委員会)は、これらの権限に時間的な制限を設けていません。その結果、傍受は、傍受を実施する機関が決定する限り続く可能性があります。

第 97 条(Ka)において認められた、国家安全保障と公の秩序を理由とする広範な権限により、政府は電気通信事業者に対して、特定のユーザーの通信に関する記録を保存するよう要求することができます。しかし、保存要求を行うかどうかを検討する際、関連する政府機関は、情報を保存するための事業者の技術的資源と能力を考慮する必要があります。

V. データ保護機関

データ保護機関がある場合は、名称と住所をご教示下さい。

デジタル・セキュリティ法のもと、ナショナル・デジタル・セキュリティ・カウンシルには、必要に応じてデータ保護ガイダンスを策定し、発行できる権限が委ねられています。ただし、コンテンツのブロックやデータソースの復号化などの実行事項については、デジタル・セキュリティ・エージェンシーが実行権限を有しています。しかし、これらは一般的な政策や内部統制に関する行政機関です。一般的に、通常の法執行機関は、対象事項の運用面の監督が委任される機関となります。