February 2022

POLICY BRIEF: Nine steps to protect our data and privacy in Sri Lanka

Sri Lanka's Personal Data Protection Bill, 2021

February 2022

This policy brief is an Access Now publication. It is written by Jade Lyngdoh, Raman Jit Singh Chima, and Namrata Maheshwari. We would like to thank the Access Now team members who provided support, including Estelle Massé.

Introduction

In January 2022, Sri Lankan lawmakers introduced the Personal Data Protection Bill in Parliament. The Bill is expected to be passed during the ongoing session of Parliament. Sri Lankan lawmakers first drafted data protection laws in 2019, when the Act to Provide for the Regulation of Personal Data Processing was published. Following that, in September 2021, the authorities presented a new version, known as the Act to Provide for Regulation of Personal Data Processing (2021). The final version of the proposed legislation was published in Sri Lanka's Gazette in November 2021.

The publication of Sri Lanka's data protection legislation coincides with the introduction of similar legislation in other South Asian nations. A new version of Pakistan's data protection law, Personal Data Protection Bill, 2021, has been published by lawmakers. In India, MPs recently published a parliamentary committee report on recommendations for the country's proposed legislation, known as the Personal Data Protection Bill, 2019.

What is data protection, and why is it important for Sri Lanka?

Data protection can be defined as the practices, safeguards, and binding rules put in place to protect people's personal information and ensure that we remain in control of it. The person utilising public or private services should be able to choose whether or not to disclose information, should be informed about their rights, including who will have access to the shared information, and under what conditions that access is allowed.

Data protection is important for upholding the human rights of Sri Lankan citizens in an ever evolving digital world, as well as to ensure resilient cyber security infrastructure. Sri Lanka is a signatory to the International Covenant on Civil and Political Rights, the International Convention on the Protection of All Migrant Workers and Members of Their Families, the Convention on the Rights of the Child, and the Universal Declaration of Human Rights. Articles of these (17, 14, 16 and 12 respectively) conventions recognise privacy as a human right, and Sri Lanka is bound by its obligations in international law to protect this right. To protect people's rights in Sri Lanka, it is imperative for the government to implement a data protection framework centered on people's privacy.

The importance of data protection is further underscored by the Sri Lankan government's digital policies, including policies to facilitate data transfers and its commitments to the Council of Europe Budapest Convention on Cybercrime. For instance, the enactment of legislation which protects individuals and organisations, and raising awareness and empowering citizens to defend themselves against cyberattacks are two key pillars of the Sri Lankan Information and Cyber Security Strategy. Additionally, a robust data protection legislation would be necessary to facilitate any future assessments for an adequacy decision under the European Union General Data Protection Regulation (GDPR). And correspondingly, alongside enacting a data protection law, we recommend that Sri Lanka

sign on to the specialised instrument of the Council of Europe, namely its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as modernised recently in 2018 (popularly referred to as Convention 108 Plus).

The importance of data protection as part of Sri Lankan policy is also reflected in the President's recent address to Parliament. The President noted that as part of rapid digitalisation and in line with the government's policy to encourage innovation and foreign investment in the technology industry, a data protection legislation has been approved by the country's cabinet. To truly fulfill these objectives, Sri Lanka needs a rights-respecting, comprehensive data protection legislation.

Why do we need comprehensive privacy laws?

Comprehensive data protection laws address current and future societal challenges while also safeguarding our fundamental right to privacy and other protected human rights. This is due to two major factors.

First, as the digital age continues to advance, laws must evolve to ensure adequate protection of human rights in a changing environment. The digital environment is rapidly changing and lawmakers must ensure that legislation keeps up with these rapid developments. For instance, the development and deployment of facial recognition technology for purposes including law enforcement has led to privacy concerns. Legislation must keep up with such developments to ensure that the rights of citizens are protected in all circumstances.

Second, corporate co-regulation and self-regulation are ineffective in protecting our data. Attempts by technology companies and other entities to establish non-binding mechanisms have not demonstrated success in tackling the issues we face. For example, the now disturbingly regular, and ever increasing large number of data breaches are but one demonstration of the need for binding obligations in the area of data security and data protection.

Based on Access Now's guide for the development of a data protection legislation, which using the learnings from the negotiations of European Union's General Data Protection Regulation and related global legal frameworks, a legislation must incorporate the following "Dos and Don'ts" recommendations, to be considered comprehensive:

DO:	**DO NOT:**
1. Incorporate a list of binding data protection principles in the legislation 2. Include a list of binding rights in the law which we can exercise without restrictions 3. Ensure transparent and inclusive negotiations when the legislation is being drafted 4. Define a clear basis under which our data can be processed 5. Define a clear scope of application for the legislation 6. Protect our data security and integrity 7. Develop a mechanism to prevent and notify data breaches 8. Establish independent authorities and mechanisms to enforce the legislation 9. Establish a secure, transparent, and binding mechanism under which data is transferred to third countries 10. Continue to uphold data protection and security	1. Seek broad exemptions for national security 2. Authorise companies to process personal data based on "legitimate interests" without strict limitations on such processing 3. Develop a "right to be forgotten" 4. Authorise companies to collect sensitive data without consent 5. Favour self-regulation and co-regulation mechanisms

Key Areas of Concerns in the present Bill and Recommendations

1. **Establishment of an independent Data Protection Authority ("DPA")**: Clause 28(1) provides that the Government may designate "a public corporation, statutory body or any other institution established by or under any written law and controlled by the government" as the Data Protection Authority of Sri Lanka. True and meaningful independence of the DPA from the executive branch and ministerial control is crucial to ensure that the DPA effectively implements the data protection legislation and upholds people's rights - particularly since the government and public sector agencies are also prominent data collectors and processors. Further, a corporation would be susceptible to conflicts of interest, and the aim of a DPA is not to make profit, thereby making it difficult to reconcile its role with that of a corporation.

Access Now recommends that the Bill be amended to ensure complete and unequivocal independence of the DPA, including in the composition, appointment, functioning, and policy framing process of the authority. **RECOMMENDATION**: Do not pass; needs amendments.

2. **Too many important issues left for subsequent rulemaking instead of being set by Parliament: Firstly**, the bill presently provides for excessive rule-making accorded to authorities: Clauses 26; 44, 12(2), 18(2)(b)), 23(1)); 27(5)); and 30(q)) each confer rule-making powers to the Government or the DPA. While provisions for rulemaking may be required in some circumstances, there is a need to ensure that such provisions are not misused - and ideally, as much as possible should be specified in the parent statute itself. **Additionally,** the issue of the independence of rulemaking by the DPA is hampered by requirement of approval from the Government; Clause 43 provides that the DPA shall enact rules, but subsection (5) of the clause requires that "a rule made under this section shall not have effect until it is approved by the Minister and approved rules and notification of such approval are published in the Gazette." This undermines the independence of the DPA in matters where its rules may place tighter controls on the government, if the Minister chooses to not approve a proposed rule with no explanation.

In light of this, Access Now recommends that the bill text should be revised to reduce the excessive rulemaking authority, and include as many clauses in this primary statute itself. For example, the rulemaking provisions in Clause 23(1) which provide for the manner, form, and time period for personal data breach notifications should be drafted into the primary legislation itself, rather than left for future rulemaking. Wherever it is demonstrated that specific matters are required to be left to future rulemaking provisions are necessary, such rules shall be subject to Parliamentary approval or other meaningful oversight such as a notice-and-comment process. Further, the bill should ideally be amended to provide for a notice and comment period upon publication of any Rules prepared by the DPA, when the Minister Minister may submit any comments or objections; and the Minister should not have the final say on whether the rules may be enforced, in order to ensure independence of the DPA. In any event, at the very least, subclause (5) of clause 43 should be amended to ensure that the

Minister may disapprove the rules only in the rarest and narrowly defined circumstances, and the Minister must be required to explain, in a published decision, when a rule proposed by the DPA is not granted approval. **RECOMMENDATION:** Do not pass; needs amendments.

3. **Data adequacy decisions made by Government**: Clause 26(1) provides that a public authority can only process personal data in a third country after receiving a data adequacy decision. Clause 26(2) lays that such an adequacy decision shall be made by the Minister "in consultation with the Authority". Clause 26(2)(b)(i) further states that such an adequacy decision may be reviewed by the Minister at least every two years.

Access Now recommends as follows: Such consultation with the DPA should be binding and should mandate written submissions of objections or assessments; these submissions must be accessible in public domain. The adequacy decision issued by the minister under the draft Bill should be published in the country's official gazette. Further, when the review of the adequacy takes place according to the draft Bill, such review should take place in consultation with the DPA, and further include a public call for evidence and consultation. When such an adequacy decision under the draft bill has been reviewed and accepted, the adequacy decision, with reasoning, must also be published in the country's official gazette. **RECOMMENDATION**: Room for improvement; needs work.

4. **Exemptions, restrictions and derogations prohibited unless they are necessary and proportionate, and protect fundamental rights and freedoms**: Clause 35 provides for exemptions, restrictions or derogations. It lays down that exemptions, restrictions or derogations must be prescribed by regulations, and respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society. Further, it sets out purposes for which such exemptions may be prescribed.

Access Now welcomes the explicit commitment in this provision to the necessity and proportionality standard, and recommends that to further strengthen the provision, "respects the essence of fundamental rights and freedoms" be changed to "respects and protects fundamental rights and freedoms" in order to make it an enforceable and objective standard for legal scrutiny. In addition, people shall be informed of these exceptions and of possible avenues for remedies, when available. **RECOMMENDATION**: Welcome with amended language.

5. **Reduced penalty provisions will impede effectiveness of law**: Clause 33(1) provides for a maximum penalty of 10 million rupees for each instance of non-compliance, which could be doubled for non-compliance under clause 33(2). The penalty has been significantly reduced since the previous draft of the data protection bill. The previous draft provided for a fine up to 2% of the global turnover (or 25 million rupees, whichever is larger) of the company which committed a breach.

Access Now recommends that the language for penalties which was present in the previous draft of the legislation replace the current text in order to ensure effective deterrence. **RECOMMENDATION:** Do Not Pass: needs amendments.

6. **Incomplete list of binding-rights**: Part II of the draft contains a list of users-rights, including the right to access [clause 13]; the right to object [clause 14]; right to rectification [clause 15]; right to erasure [clause 16]; grant or refusal of rectification, completion, erasure or refrain from further processing [clause 17]; right to review automated individual decision making [clause 18]; and the right of appeal to DPA [clause 19]. While these are welcome provisions, lawmakers must incorporate additional rights into the legislation.

Access Now recommends that the following rights be incorporated to Part II: the right to information; the right to explanation; the right to portability; and the right for representative associations or public interest groups to file on behalf of individuals, especially those from challenged or vulnerable communities. Further, the provisions in Clause 19(3) must include a statutory time-period of no more than 6 months for the completion of the investigation by the DPA of an appeal. **RECOMMENDATION**: Not satisfactory; needs amendments.

7. **No notifications to citizens in the event of a personal data breach**: The provisions in clause 23 only mandate a notification to the DPA in the event of a personal data breach, and not to a user. To ensure transparency and accountability, and that the rights of citizens are upheld, it is necessary for users to be notified in the event of such personal data breach.

Access Now recommends that the Bill be amended to incorporate a mandate for users to be notified on the occurrence of a personal data breach. Furthermore, a breach notification period should be included. We recommend that a breach shall be notified to DPA no later than 5 days after its discovery and then rapidly to citizens with recommendations on how to protect their information following the breach. **RECOMMENDATION:** Do not pass; needs amendments.

8. **Protection of data must not come at the cost of people's right to information**: Clause 45 of the Bill on "official secrecy" requires officers appointed to the DPA to swear to "observe strict secrecy" in respect of information that comes to their knowledge, unless compelled by a court order or for compliance with applicable laws. The need to protect information must be balanced with people's right to information. The former has often been used as an excuse to deprive people of access to information citing broad claims of official secrecy and national security. Access Now recommends that appropriate language be inserted in Clause 45 highlighting that people's right to information must be prioritised, principles of necessity and proportionality must be followed, and where access is denied on grounds of official secrecy or other state interests, the DPA must provide reasons in writing. The applicant must have the right to challenge the decision in court. We emphasise that such provisions

make it even more imperative that the DPA is completely independent of any direct or indirect government control.

9. **Exclusion of data processing by any actors set up under written law in Sri Lanka or entities acting under the Code of Criminal Procedure**: Schedule IV of the Bill provides a disproportionately wide exception for processing relating to investigations of offences or related security measures. It provides that processing of personal data may be considered lawful if investigations are carried out pursuant to the Code of Criminal Procedure Act or any other law, and safeguards may be prescribed.

Access Now recommends that strict limitations and safeguards must be incorporated in the Schedule. In order to prevent misuse and abuse of the exception, to the detriment of people's rights, such safeguards and limitations must be treated as a prerequisite, and an effective oversight mechanism just be established. It is recommended that the Bill be amended to incorporate safeguards including the following: (a) agencies that need to process data for purposes mentioned in Schedule IV must register with the DPA and provide details regarding its data collection, storage and disclosure processes and the specific needs that they serve; (b) agencies must be required to seek the DPA's approval to exercise its processing powers under Schedule IV; (c) The DPA must periodically publish a report in the public domain with details of the number of times each agency utilised the Schedule IV exemption, the purpose for each instance, and other relevant details; (d) people must have the right to file complaints before the DPA and be heard with respect to any grievance arising from Schedule IV and the DPA must have the necessary enforcement powers. Further, Schedule IV must be subject to a review within two years to assess use cases, and substantive as well as procedural propriety. **RECOMMENDATION:** Serious concerns; needs work.

Summary Recommendations

1. **Establish a Data Protection Authority which is completely independent of the Government.** AMEND CLAUSES 28, 43.
2. **Rule-making powers conferred on the government and the DPA should be limited. Ideally, the Minister should submit objections during a "notice and comment" on publication of the rules. At the very least, a written explanation by the Minister must be necessary when a rule proposed by the DPA is not granted approval, which must be permitted only in narrowly defined circumstances.** AMEND CLAUSES 26, 44, 12, 18, 23, 27, 30, 43.
3. **Build transparency into the legislation with respect to the process of making an "adequacy decision" for data flows.** AMEND CLAUSE 26.
4. **Apply the strict standard of necessary and proportionate and ensure protection of fundamental rights and freedoms in the context of any exemptions, derogations or restrictions that may be prescribed.** AMEND CLAUSE 35.
5. **Penalties for entities that breach data protection legislation should not be reduced.** AMEND CLAUSE 33.
6. **Incorporate additional rights for the users into the Bill.** AMEND CLAUSE 17, 19(3).
7. **Notify users in the event of a personal data breach.** AMEND CLAUSE 23.
8. **Official secrecy or protection of information for state interests must not be at the cost of people's right to information.** AMEND CLAUSE 45.
9. **Impose safeguards and limitations, and provide for oversight, on the exemption for data processing for investigation and security measures, to protect people's rights and ensure transparency and accountability.** AMEND SCHEDULE IV.

In addition to our detailed and summary recommendations, policymakers should consult our guide to comprehensive data protection legislation as they continue to debate the Regulation of Personal Data Processing, 2021 Bill in Parliament. The guide was developed using the learnings of what to do and not do from the European Union General Data Protection Regulation and related global legal frameworks.

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For more information, please contact:

Namrata Maheshwari | Asia Pacific Policy Counsel | namrata@accessnow.org

Raman Jit Singh Chima | Senior International Counsel and Asia Pacific Policy Director | raman@accessnow.org