Data Governance Framework: Sri Lanka

Data for Development — South and Southeast Asia

Ashwini Natesan & Chiranthi Rajapakse

October 1, 2025

Table of contents

List of figures

List of tables

List of abbreviations

AI	Artificial Intelligence
AIC	Asia Internet Coalition
APTA	Asia-Pacific Trade Agreement
CBSL	Central Bank of Sri Lanka
CI	Critical Information
CINTEC	Computer and Information Technology Council of Sri Lanka
COMPOL	National Computer Policy
CRIB	Credit Information Bureau of Sri Lanka
CSA STAR	Cloud Security Alliance Security, Trust, Assurance and Risk Program
CeSP CSP	Certificate Service Provide Cloud Service Provider
DCS	Department of Census and Statistics
DIPA	Digital Infrastructure Protection Agency
DPA	Data Protection Authority
DRP	Department of Registration of Persons
DSZ	Digital Sovereignty Zones
EMV	Europay, Mastercard, Visa
ETA	Electronic Transactions Act
EU	European Union
FGDs	Focus Group Discussions
FOSS	Free and Open Source Software
FTA	Free Trade Agreement
GAIA-X	European Data Infrastructure Initiative (France and Germany)
GIC	Government Information Center
GoSL	Government of Sri Lanka
GovPay	Government Unified Digital Payments Platform
HR	Human Resources
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Agency of Sri Lanka
IDRC	International Development Research Centre
ISO	International Organization for Standardization
ISO/IEC 27017	International Standard for Cloud Security

KYC	Know Your Customer
LGC	Lanka Government Cloud
LGN	Lanka Government Network
LGPS	Lanka Government Payment Service
LIFe	Lanka Interoperability Framework
LIS	Land Information System
LNDX	National Data Exchange (NDX)
MOSIP	Modular Open Source Identity Platform
MOU	Memorandum of Understanding
MP	Member of Parliament
MPAs	Marine Protected Areas
NARESA	Natural Resources, Energy and Science Authority of Sri Lanka
NDX	National Data Exchange
NFP	National Fuel Pass
NIC	National Identity Card
NIST	National Institute of Standards and Technology
NSDI	National Spatial Data Infrastructure
OGP	Open Government Partnership
OSA	Online Safety Act
OSM	Open Street Maps
PA	Public Authority
PDPA	Personal Data Protection Act
PUF	Public Use Files
QR code	Quick Response Code
R&D	Research and Development
RTI	Right to Information
RTIC	Right to Information Commission
SAARC	South Asian Association for Regional Cooperation
SAFTA	South Asian Free Trade Area
SL	Sri Lanka
SL CERT	Sri Lanka Computer Emergency Readiness Team
SL-GEA	Sri Lanka Government Enterprise Architecture
SLSD	Sri Lanka Survey Department
SLSI	Sri Lanka Standards Institute
SMEs	Small and Medium Enterprises

UN	United Nations
UN ECC	United Nations Electronic Communication Convention
UNCITRAL	United Nations Commission on International Trade Law
UNDP	United Nations Development Programme
VPN	Virtual Private Network

About this report

About LIRNEasia

LIRNEasia is a pro-poor, pro-market regional policy think tank. Our mission is *Catalysing policy change and solutions through research to improve the lives of people in the Asia and Pacific using knowledge, information and technology.*

Address: 15 2/1, Balcombe Place, Colombo 8, Sri Lanka.
Telephone: +94 11 267 1160
Email: info@lirneasia.net
Website: https://lirneasia.net/
Twitter: https://x.com/LIRNEasia
Facebook: https://www.facebook.com/lirneasia/
YouTube: https://www.youtube.com/@LIRNEasia-
LinkedIn: https://lk.linkedin.com/company/lirneasia
Instagram: https://www.instagram.com/lirneasia/

Funding

This work was carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada. The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

1 Introduction

This report on data governance in **Sri Lanka** is part of the "Harnessing Data for Democratic Development in South and Southeast Asia" (D4DAsia) project, which aims, *inter alia*, to create and mobilize new knowledge about tensions, gaps, and the evolution of the data governance ecosystem, taking into account formal and informal policies and practices.

In today's digital age, data governance ecosystems play a crucial role in shaping our societies. These ecosystems, comprising policies, laws, practices, behaviors, and technologies, aim to govern data in ways that protect rights, foster innovation, enhance transparency, and ultimately promote democratic and inclusive governance. However, the landscape of data governance is complex and often fraught with challenges, particularly in South and Southeast Asia.

A data governance ecosystem comprises the policies, laws, practices, behaviors, and technologies that govern data. An ideal data governance system would protect rights, enable innovation, enhance transparency, and contribute to achieving democratic and inclusive governance. Throughout the remainder of the report, unless the context indicates otherwise, the term "policies" is used as shorthand for policies, statutes, regulations, rules, administrative orders, and even practices and technologies used to implement these as part of the data governance ecosystem.

Data is increasingly being recognized as an enabler for development. It is an essential requirement for policymaking and monitoring of development goals and targets. When effectively managed, data can be used as an asset to support significant development actions such as poverty reduction, food security, mitigating the impact of climate change, and disaster management. If mismanaged, it can exacerbate inequalities and undermine the development potential of the same actions.

The D4DAsia project has produced nine reports so far — seven detailed individual country reports which deal with the issues of data governance in the following countries: India, Indonesia, Nepal, Pakistan, Philippines, Sri Lanka and Thailand; a detailed look at data protection in South Korea; and a synthesis report that summarizes the findings from the various countries while drawing out the contrasts amongst them, along with detailed findings to the research questions we posed, which were:

1. What is common, and what is nationally specific, in the emerging data governance architectures in South and Southeast Asia? What are the explanations?
2. What are the implications of the emergent nature of the governance architecture? Because there is no overall design that envisions how the parts fit together, it is likely that there will be friction points and even contradictions. How are these being worked out?
3. The emerging governance architecture involves trade-offs among objectives such as greater accountability of powerholders, economic growth, including the creation of employment and wealth, resilience of systems, etc. How have different societies: (a) explicitly recognized the trade-offs or not; and (b) handled them?
4. Are there legislative or policy innovations with potential for replication? What are the modalities of sharing experiences? Are developing countries learning from each other, or are they learning from the developed countries?

5. How were the laws and bills developed? What expertise was brought to bear? How open were the procedures? How receptive were drafters to suggestions and criticisms?
6. How were capacity challenges addressed: by simplifying the laws or by tolerating incomplete implementation?

1.1 Structure of the report

1.1.1 Governance background

The report starts by providing contextual information about the constitution and governance framework in **Sri Lanka**, including how lawmaking powers are distributed and delegated, the powers of the judiciary to overturn laws or to enforce policies, and the legal and regulatory background in the country.

1.1.2 Increasing openness / access

The report then discusses policies that increase openness or access. By this, we mean policies that allow greater access by citizens, consumers, and corporations to data, or facilitate interoperability or cross-border data transfer. Specifically, we do not include increased governmental access to citizens' private data or non-public corporate data.

This section discusses open data policies, the question of how much governmental data is made available proactively, and how much is reactive as well as the quality of data being disseminated. The report also assesses government policies favoring or requiring free and open source software (FOSS) or open standards, noting any specific standards that are mandated.

1.1.3 Decreasing openness/access

The report then moves on to discuss the opposite, i.e., laws, policies, and practices which decrease openness or access. By this we mean decreasing access of citizens, consumers, and corporations to data. To be clear, this is not a negative value judgement, since upholding important individual and collective rights, such as privacy and public security, necessitates reducing citizens' access to data.

This theme explores issues of security, such as whether there are any data retention or localization requirements, restrictions on the right to access information (such as national security, privacy, etc.) and exceptions to data security requirements for law enforcement. We further discuss the privacy and copyright framework in brief and specifically try to answer whether there are any exceptions for search engines as well as for research and artificial intelligence (AI).

The issue of data governance and the policies surrounding its implementation is critical for governments, citizens, and businesses across the world. As mentioned earlier, we use the term data governance to refer to "diverse arrangements, including technical, policy, regulatory or institutional provisions, that affect data and their creation, collection, storage, use, protection, access, sharing and deletion across policy domains and organizational and national borders."[1]

[1] OECD, *Going Digital Guide to Data Governance Policy Making.*

2 Background

2.1 Legal Foundation

The legal system of Sri Lanka is influenced by the legal traditions of civil and common law systems.[2]

The statutory laws of the country have English law origins, while Roman-Dutch law is the residuary law of the country. Lord Diplock, in the case of *Kodeeswaran v. Attorney General,* termed case laws the "indigenous common law of Sri Lanka."[3] The Constitution of Sri Lanka is an amalgamation of the Westminster model with the French Presidential system. There is an executive President with powers in addition to the Prime Minister and Parliament.[4] Since gaining independence in 1948, Sri Lanka has had three Constitutions.[5] The 1978 Constitution, which is currently in force, provides an Executive Presidential System of Government with a Prime Minister playing a relatively minor role.[6] In 2015, the 19th Amendment to the Constitution altered the role of the Executive President in certain respects, for example, the President could no longer remove the Prime Minister, and dual citizens were prohibited from serving as Members of Parliament. The powers of the President were also restricted in the ability to dissolve the Parliament, and appointments for certain high-level positions had to be made only with the concurrence of the Constitutional Council.[7] While the 20th Amendment had reversed many of these changes, the 21st Amendment rolled back most of those.[8]

2.1.1 The Constitution of Sri Lanka

Article 14 (1) (a) of the Constitution enshrines the fundamental right of speech and expression, including publication.[9] Article 15 (2) holds that the right is subject to "such restrictions as may be *prescribed by law* in the interests of *racial and religious harmony or relation to parliamentary privilege, contempt of court, defamation or incitement to an offence"* (emphasis added).[10] Freedom of expression can also be restricted '…as may be prescribed by law in the interests of national security, public order and the protection of public health or morality, or to secure due recognition and respect for the rights and freedoms of others, or of meeting the just requirements of the general welfare of a democratic society'; Article 15 (7) The Article also specifies that 'law' includes 'regulations made under the law for the time being relating to public security.' Commentators have criticized the fact that Article 15 does not specify conditions such as 'necessity', 'reasonableness', or 'justifiability' in imposing restrictions.[11]

---

2 Cooray, *An introduction to the legal system of Sri Lanka.*
3 *72 NLR 337.*
4 Cooray, *An introduction to the legal system of Sri Lanka.*
5 Cooray.
6 Perera, *Semi-Presidentialisation and Executive Accountability: A Cautionary Tale from Sri Lanka to the UK.*
7 Constitution of the Democratic Socialist Republic of Sri Lanka, 19th Amendment.
8 Constitution of the Democratic Socialist Republic of Sri Lanka, 20th and 21st Amendments.
9 Constitution of the Democratic Socialist Republic of Sri Lanka.
10 Constitution of the Democratic Socialist Republic of Sri Lanka.
11 Gunatilleke, *A Rights-Based Approach to Limitation Clauses in the Sri Lankan Constitution.*

The above provisions allow for restrictions "prescribed by law," and in Sri Lanka, judicial review of laws is limited to before the Bill becomes an Act. Once the legislative process is complete, there is no judicial review, i.e., no post-legislative review (Article 80(3) of the Constitution).[12] Furthermore, Article 16(1) states that all existing written laws and unwritten laws are valid and operative, notwithstanding any inconsistency with the provisions of the Chapter of the Constitution on Fundamental Rights.

This does not mean that the Supreme Court of Sri Lanka has not delivered decisions of grave importance and exercised its powers in several landmark cases. The determination made by the Supreme Court in the *Sri Lanka Broadcasting Authority Bill* (SC/SD llll997-1511997), is an example of the use of its judicial review powers.[13] In the recent past, the Supreme Court decision of *Mohamed Razik Mohamed Ramzy v. B.M.A.S.K. Senaratne* is a landmark one.[14] Remarking on the necessity to safeguard the fundamental rights under Article 14, Justice Yasantha Kodagoda, stated as follows:

"Long-term suppression of the fundamental rights contained in Article 14, coupled with systematic and widespread erosion of the rule of law guaranteed by Article 12, supplemented by gross infringements of Articles 11 and 13 rights, augmented by the inability to meaningfully and effectively exercise the right to information recognized by Article 14A, is a recipe for the eruption of serious consequences."[15]

Despite these examples, once legislation is passed, it cannot be amended or struck down by judicial intervention. In the recent example of the Online Safety Act No. 09 of 2024, there were allegations that the amended version did not contain all the changes as envisaged in the Supreme Court Determination.[16] The Supreme Court dismissed the fundamental rights petition challenging the certification by the Speaker. The objection of the Attorney General that the Supreme Court had no jurisdiction was accepted. The Supreme Court observed that the legislature had intentionally ousted the jurisdiction of courts and tribunals, not only reviewing the legislation passed by Parliament but also the legislative process in enacting legislation on any ground, and that Articles 80(3) and 124 of the Constitution have prevented the post-legislative scrutiny of Acts passed by Parliament.

2.2 Digital Governance Landscape

A plethora of national policies and frameworks have been drafted concerning the governance of data and information. These have also included various institutional mechanisms to implement policies.

The first policy to outline the importance of Information and Communication Technology was the National Computer Policy (COMPOL) of 1983. This first attempt was taken by the Natural Resources, Energy, and Science Authority of Sri Lanka (NARESA) under the instructions of the then-President. A committee appointed by NARESA produced the 'National Computer Policy'. Subsequently, the Computer and Information Technology Council of Sri Lanka (CINTEC) was established by the Computer and Information

12 *Daily FT*, "The rule of law."
13 Supreme Court Sri Lanka Broadcasting Authority Bill.
14 **MohamedRazikMohamed2023?**
15 *Mohamed Razik Mohamed Ramzy v. B.M.A.S.K. Senaratne.*
16 LBO, "Online Safety Act."

Technology Council of Sri Lanka Act No. 10 of 1983 and later renamed as the Council for Information Technology to function directly under the then President by the Computer and Information Technology Council of Sri Lanka Act[17] No. 10 of 1984.

The Information and Communication Technology Act No. 27 of 2003 ("ICT Act") provides for the establishment of the Information and Communication Technology Agency of Sri Lanka (ICTA), which replaced CINTEC as the country's apex ICT institution[18] .[19] In terms of the ICT Act, ICTA has been mandated to take all necessary measures to implement the Government's Policy and Action Plan concerning ICT.[20] Specifically, in accordance with Section 6 of the ICT Act, ICTA is required to assist the Cabinet of Ministers in formulating the National Policy on ICT and provide all necessary information for its development. ICTA was established as a company wholly owned by the Government of Sri Lanka for five years with a specific 'sunset clause.'[21] However, the Act was amended in 2008, allowing it a permanent existence and mandating it to take all necessary measures to implement the Government's Policy and Action Plan related to ICT.[22]

Sri Lanka passed the Electronic Transactions Act No. 19 of 2006 (ETA) based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996) and Model Law on Electronic Signatures (2001). It provides for functional equivalence to electronic contracts and signatures with those of paper-based/handwritten. It also enables the legal recognition of electronic record retention and the admissibility of electronic evidence in courts of law.[23] The ETA was amended in 2017 to harmonize with the UN Electronic Communication Convention (UN ECC), particularly to facilitate the signing of contracts virtually across national borders.[24] Section 23 of the ETA provides restrictions on the application of the legislation. Notably, this excludes financial transactions, including foreign exchange transactions and those relating to settlements and payments. It could be argued that this is to protect against regulatory conflict with the Central Bank of Sri Lanka and the requirements imposed by relevant enactments, including the Foreign Exchange Act. However, no equivalent requirements have been imposed under the sector-specific regulations. This has resulted in a regulatory lacuna.

2.2.1 Policies issued by ICTA

The Cabinet approved the first e-Government policy of Sri Lanka in December 2009, and it was to be adopted and implemented by all government organizations from 2010 to 2012. The Cabinet of Ministers gave ICTA the mandate to monitor the implementation, review the policy, and revise it as necessary. The said policy, among others, provided for easy access to government information electronically by citizens, as well as online access to government services. Despite its lofty ideals, a review by ICTA showed that the

---

17 **parliamentofthedemocraticsocialistrepublicofsrilankaComputerInformationTechnology1984?**

18 "Information and Communication Technology Agency of Sri Lanka."

19 **parliamentofthedemocraticsocialistrepublicofsrilankaInformationCommunicationTechnology2003?**

20 **parliamentofthedemocraticsocialistrepublicofsrilankaInformationCommunicationTechnology2003?**

21 Information and Communication Technology Act No. 27.

22 **parliamentofthedemocraticsocialistrepublicofsrilankaInformationCommunicationTechnology2003?**

23 **ElectronicTransactions2006?**

24 Electronic Transactions Act Amendment 2017.

implementation was low.[25]

According to a Circular issued by the Presidential Secretariat in 2020, the ICTA was tasked with driving the Government's National digital initiatives.[26]

Currently, the 'National Policy Framework' of Sri Lanka, under its three main pillars of Digital Government, Digital Economy, and Digital Services, is said to lay the foundation for transforming the country into a technology-based society. ICTA's Policy Division provides the direction and guidance needed by the government in its 'Digital Transformation.'[27] Figure 1 below depicts this.

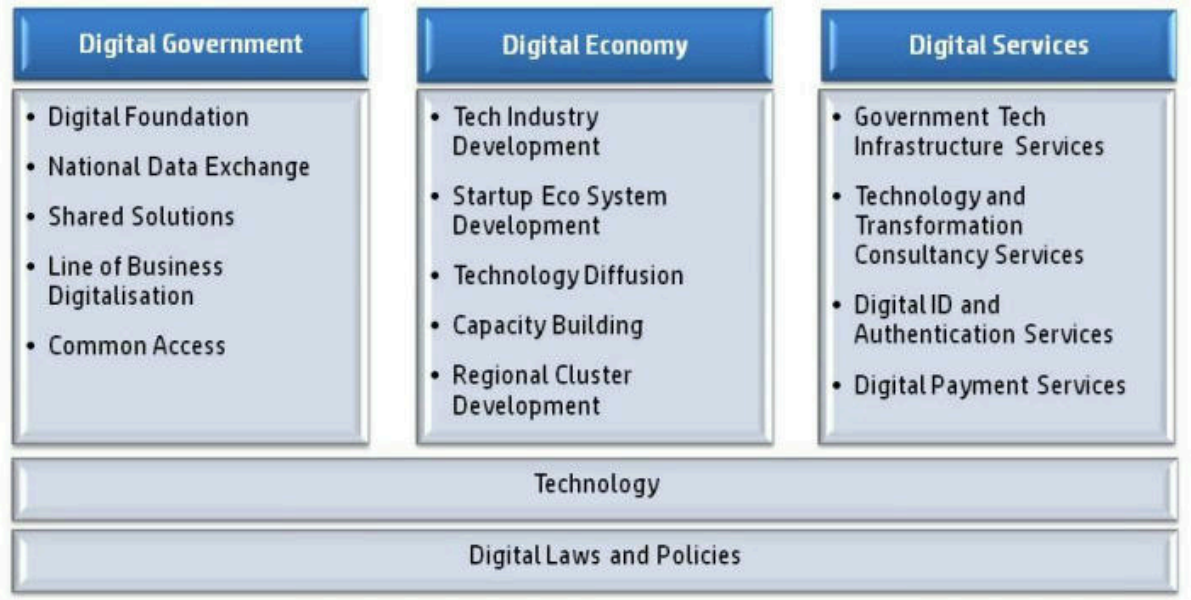

Figure 1: National Policy Framework for Digital Transformation

Source: ICTA Policy Division.[28]

However, a policy directive of the Cabinet of Ministers in May 2024 states that ICTA will be absorbed by a 'Digital Transformation Authority' under a new law being drafted, thus vesting it only with the responsibilities of policy and strategy aspects. In contrast, ICTA has previously been engaged in activities ranging from policy development to project implementation.[29] By a gazette notification in November 2024, the Ministry of Digital Economy was created, *inter alia,* the newly created Ministry will be responsible for

1. Policy formulation and supervision of critical institutions such as Sri Lanka Telecom, ICTA, Data Protection Authority, SL CERT,
2. cyber security, digital forensics, and building digital trust.
3. Implementation of laws like the Personal Data Protection Act (2022) and ICT Act (2003) to ensure secure and efficient governance. The Registration of Persons Act,1968, is also included (presumably to enable digital ID).

---

25 E-Government Policy- Draft.
26 Presidential Secretariat, "PSGPACircular."
27 "Information and Communication Technology Agency of Sri Lanka."
28 **PolicyInformationCommunication?**
29 Fernando, "New Digital Transformation Agency to Absorb ICTA."

2.3 Increasing openness/access

2.3.1 Right to Information Act No. 12 of 2016

The right to information (RTI) is guaranteed as a fundamental right by Article 14A of the Constitution of Sri Lanka.[30]

The Right to Information Act No 12 of 2016 ("RTI Act") was passed unanimously by the Parliament on 4th August 2016.[31] It commenced operationalization on 3 February 2017.[32] The enactment and implementation of the RTI Act, together with the establishment of the RTI Commission soon after, fulfilled one of the first 13 Open Government Partnership (OGP) Commitments made in 2016, when Sri Lanka became the OGP's 68th signatory. The passing of the RTI Act remains a landmark in the country's public governance history. Regrettably, Sri Lanka lost its OGP membership in June 2025 due to failure to deliver the action plan from the 2019-2021 cycle.[33] In a global ranking, the Sri Lankan RTI Act has been ranked fourth in the world, based on the provisions and safeguards it provides under the Act.[34]

The RTI Act provides for disclosure of information that is in possession, custody or control of a "public authority".

The term "public authority" has been widely defined. The definition also includes private organizations as follows (Section 43): "a private entity or organization which is carrying out a statutory or public function or service, under a contract, a partnership, an agreement or a license from the government or its agencies or from a local body, but only to the extent of activities covered by that statutory or public function or service". Similarly, private educational institutions have also been included under the definition. Non-governmental organizations substantially funded by the government or foreign government(s), or international organizations would come within the scope of "public authority" insofar as they provide a service to the public.

The RTI Act has an overriding effect over other legislation, wherein, in the event of inconsistency between the RTI Act and another law, the former prevails (Section 4 of the RTI Act). Section 3 of the RTI Act empowers citizens to access any information which is in the "possession, custody or control of a public authority."

Another noteworthy provision of the RTI Act is that under Section 35, the officer / public authority is required to give reasons for arriving at a decision on the information request. Section 40 of the RTI Act protects an officer/employee of the public authority from any punishment or disciplinary action for disclosing information permitted under the Act.

---

30 Constitution of the Democratic Socialist Republic of Sri Lanka.

31 Right to Information Act, No. 12 of 2016.

32 Right to Information Act, No. 12 of 2016.

33 *Times Online*, "Sri Lanka loses its membership of the Open Government Partnership."

34 Centre for Law and Democracy and Access Info Europe, *Global Right to Information Rating*.

2.3.2 National Archives Law No. 48 of 1973 (as amended) ("National Archives Law")

The National Archives Law provides for the establishment of the Department of National Archives, for the transfer of public records to the archives and lays down provisions for the custody and preservation of public records.[3536]

In terms of section 9(2) (b)(d) of the Archives Act, public records that are not less than twenty-five (25) years old, as required by the Director (Director General as designated presently), should be transferred to the National Archives Department for permanent preservation.[37]

Observations

As discussed in an interview with the Director General of the Department of National Archives, conflicts exist between provisions of the RTI and archiving requirements with regard to retention of records, including the following:

Section 7(3) of the RTI Act

(3) All records being maintained by every public authority shall be preserved

(a) in the case of those records already in existence on the date of coming into operation of this Act, for a period of not less than ten years from the date of coming into operation of this Act; and

(b) in the case of new records which are created after the date of coming into operation of this Act, for a period of not less than twelve years from the date on which such record is created.

Therefore, records that were created before the RTI came into effect must be kept for a minimum period of 10 years since the enactment of the Act (until 2027).

However, this provision has been widely misread by some public authorities as implying that this authorizes the destruction of records beyond the 10 or 12 years stipulated in the RTI Act section above. As a result, the section has often been used as a justification for destroying records after this period. Under the archiving regulations, the minister in charge may make regulations on how public authorities should maintain records, and no records should be destroyed without authorization through a retention schedule.

Another practical challenge is that, because of this retention requirement and the wide definition of "information" under the RTI Act, even routine documents must be kept for ten (10) years, which creates a huge administrative burden for many public authorities. Public authorities have also stated that physical storage of records proves to be a challenge.

---

35 National Archives Law, No. 48 of 1973.

36 "Public record" or "record" means "any original or copy of any manuscript, paper, letter, register, report, book, magazine, map, chart, plan, drawing, picture, photograph or any other record or part thereof either handwritten, drawn, printed or produced in any other way on paper or on any other material except granite and officially received or produced or prepared in any public office in the course of its official functions and includes any cinematograph, film, recording, tape, disc or production in any other media received in any public office. "Printed matter" means any book, magazine, leaflet, newspaper, or any other paper containing information printed by any mechanical or by any other process."

37 9 (2): "It shall be the duty of the responsible officer of any public office or any other person for the time being having custody of any public records-

Numerous gaps in the existing Archiving laws have been identified through the draft National Policy on Archives and Record Management. The paragraphs below discuss the identified gaps.

Current attempts to address policy gaps related to archiving

A draft 'National Policy on Archives and Records Management' was recently formulated by the Department of National Archives.[38] A consultative process was followed in drafting the Policy: a call for public written submissions on the policy was issued, and public hearings followed the submissions. However, the number of written submissions received from outside Colombo, the capital city was very low; as a result, hearings were limited to Colombo.[39]

The draft policy identifies many gaps and priority issues that need to be addressed and gives detailed recommendations.

Section 16 of the existing Archives Act states that the Minister in charge of the subject has the power to make regulations allowing public access to public archives and terms and conditions. The Minister also has the power to prohibit or restrict disclosure of information.[40] However, it appears that regulations regarding public access have not been recently updated: Gazette Regulations were issued in 1979 and amended in 1980.[41] According to information provided by the National Archives, these are the most recently issued regulations.

The lack of updated systems for providing digital access to information and maintaining digital records management has been identified as a gap in the existing archiving regulations. The 'National Policy on Archives and Records Management' describes this as one of the priority issues that needs to be addressed, and the Policy gives detailed recommendations on addressing it, including revising the existing Archives Act.[42]

Section 6 of the draft policy is on Digital Records and contains recommendations on digital record keeping, preservation, data security, metadata and contextual information, digital access and open data, and providing digital records training and skills.

A Committee has also been appointed to revise the existing National Archives Law. In January 2024, this Committee released the Framework for National Archives and Records Management Legislation and a public call for comments on the framework was issued.[43] The framework suggests provisions that attempt to resolve potential inconsistencies with other enactments. For instance, the framework seeks to exempt archives from certain

---

38 Draft National Policy on Archives and Records Management v 1.2.

39 Interview with Director General, Department of National Archives.

40 Section 16. The Minister may make regulations for any one or more of the purposes hereinafter prescribed: (d) public access to the public archives and the terms and conditions subject to which public archives or any specified class or description of public archives are open to inspection by the members of the public; (e) prohibition or restriction of the disclosure of information obtained by the public from public archives.

41 Public Access To Government Documents Gazette English.

42 Section 6 of the draft Policy is on Digital Records and contains recommendations on digital record keeping, preservation, data security, meta data and contextual information, Digital access and open data, and providing digital records training and skills. (Pages 6-7)

43 Framework for National Archives and Records Management Legislation.

provisions of the Personal Data Protection Act.[44] These exemptions relate to the rights of data subjects and cross-border transfer of data.

Section 22 (2) of the Framework states that Sections 14, 15, 16 and 26 of the Personal Data Protection Act, No. 9 of 2022, 'shall not apply to personal data processed for archiving purposes in the public interest to the extent that the application of those provisions would prevent or seriously impair the purposes of archiving in the public interest, including affecting the authenticity, reliability, integrity, usability and durability of archives'.

Section 14 of the PDPA applies to the data subjects' right of withdrawal of consent and objection to processing, Section 15 applies to the right to rectification or completion, Section 16 applies to the right to erasure, and Section 26 applies to cross-border data flows. However, there are also safeguards for these exemptions; the framework also states that the 'National Archivist shall make provision for any written request or letter of objection submitted by an aggrieved person in relation to their rights as data subjects to be included with the catalogue or accession record'. The framework attempts to strike a balance between allowing processing of data for archiving purposes, while also protecting the rights of data subjects.

Section 22 (3) of the Framework states that when personal data is processed for archiving purposes in the public interest, the National Archivist shall ensure the implementation of technical and organizational safeguards to protect personal data referred to in section 10 of the Personal Data Protection Act No. 9 of 2022. Section 10 states that *every* controller shall ensure integrity and confidentiality of personal data that is being processed, by using appropriate technical and organizational measures, including encryption, pseudonymization, anonymization or access controls or such other measures as may be prescribed so as to prevent the unauthorized or unlawful processing of personal data; or loss, destruction or damage of personal data. Once again, this provision attempts to allow the processing of personal data when required, while respecting the rights of data subjects.

There are also references to the RTI Act explained above. It is commendable that the framework has sought to address these inconsistencies and also opened it up for public comments.

Challenges in implementation

As discussed in an interview with the Director General of the Department of National Archives, many capacity challenges can be foreseen in putting the policy into effect. A major challenge is the lack of properly trained staff, even if the current laws and policies are updated to improve preservation of records and public access to archival materials, implementation will require staff to be trained and have adequate knowledge of these procedures. The Department is currently trying to address this situation by bringing in

[44] 22 (2) Sections 14, 15, 16 and 26 of the Personal Data Protection Act, No. 9 of 2022, shall not apply to personal data processed for archiving purposes in the public interest to the extent that the application of those provisions would prevent or seriously impair the purposes of archiving in the public interest, including affecting the authenticity, reliability, integrity, usability and durability of archives: Provided that the National Archivist shall make provision for any written request or letter of objection submitted by an aggrieved person in relation to their rights as data subjects to be included with the catalogue or accession record of the collection to which the request or objection pertains. (3) Where personal data is processed for archiving purposes in the public interest, the National Archivist shall ensure the implementation of technical and organisational safeguards to protect personal data referred to in section 10 of the Personal Data Protection Act No. 9 of 2022;

experts from other countries to provide training on archives and record management. An immediate need is to gazette retention schedules for public authorities, which would specify whether the public authorities are required to maintain a record in their office, destroy it, or transfer it to the archives. Bureaucratic and political processes have also been a challenge for a consistent administrative and operational environment, with the Department functioning under several different line Ministries in the past years.

2.3.3 Survey Act No 17 of 2002 (Survey Act)

The Sri Lanka Survey Department (SLSD) oversees surveying and mapping in Sri Lanka.[45] The Surveyor General is the head of the Department, head of the Surveying and Mapping profession, and Chairman of the Land Survey Council.

There are references to the digitization of data in both the Survey Act No. 17 of 2002 and associated regulations. The interpretation section of the Survey Act (Section 66) defines the term 'map' to include digital forms of representation. The term "map" has been widely defined, as under Sections 6 and 7 of the said Act, and aerial photography or mapping can only be carried out under the "direction and supervision of the Surveyor General." However, it appears that Google Maps or Google Street mapping in Sri Lanka was done independently by Google without government involvement.[46] Volunteers also maintain Open Street Maps (OSM- geographic databases updated and maintained via open collaboration) in Sri Lanka.[47]

The Departmental Survey Regulations (2020) apply to surveys carried out by the Survey Department and by registered licensed surveyors.[48] The section on Digital Data Management in the regulations describes how a Land Information System (LIS) is maintained for the whole country and how digital data produced in field surveys has to be shared in this system.[49] Information provided by the Survey Department website explains how data for the LIS is received through the 'Bimsaviya' Survey program implemented under the registration of the Land Title project. The data included in the LIS system includes details such as ownership and title registration details. However, as far as could be ascertained, this data is not publicly accessible in digital form.

2.3.4 Census Data

The Census Ordinance No. 9 of 1900 has substantially remained the basis for census taking in Sri Lanka throughout the years, with amendments in 1945, 1955, 1980, and 2000. Currently, this does not appear to have provisions relating to the digitization of data, etc. The Census Department's website reports that steps are being taken to amend the Census

---

45 "The Department"; Survey Act No 17 of 2002.

46 *The Sunday Times Sri Lanka*, "Google 'Maps' Launches SL Project to Show People Shops, Where They Live."

47 "Sri Lanka - OpenStreetMap Wiki."

48 Departmental Survey Regulations.

49 The regulations give guidance on how digital maps should be prepared. For example there is detailed guidance on how digital data management systems should be followed with regard to each of the following: Equipment and Software, Field Investigation and Data Collection, Building up Digital Drawing, Quality Control in Digital Drawing, Data Storage, Security and Back up, Database of Survey Requisitions, Canning of old field sheets and usage of images. Regulation 22.14 deals with "Data Storage, Security and Back up". Accordingly, all digital data related to the survey should be securely archived in the Divisional Survey Office for easy reference.

Ordinance and the Cabinet of Ministers has given approval to do the amendments as required. According to the website, amendments were sent to the Legal Draftsman's Department for drafting the new bill, which will then be submitted to Parliament.[50]

Department of Census and Statistics

The data dissemination section of the Department of Census and Statistics ("DCS") describes data dissemination as 'releasing or making available data obtained from statistical activities such as Surveys or Census to users through various forms and media.'[51] DCS provides services to the Government, its agencies, the private sector, and the general public in their data and information needs under two approaches.

Proactive dissemination

DCS provides access to the official statistical publications and datasets available on its main website electronically and from the Departmental sales counter for printed publications.[52] The DCS website has a searchable portal where users can search and download publicly available data. Though the website states that datasets are publicly available (for example, Labor survey, household income and expenditure survey), what is publicly available is the summary data, not the actual datasets. Datasets must be requested from the Department. An application must be submitted, which must include the details of the research study for which data is being requested (including a research proposal), the requesting organization, and the details of the researchers who will have access to the data. (Reactive dissemination)[53]

The Dissemination Policy on Microdata, Department of Census and Statistics of 2014 sets out the guidelines that the DCS should follow in publishing and disseminating statistical data to all users, in order to help in policy formulation and decisionmaking.[54] The policy states that all designated official statistics, either solely produced by DCS or in cooperation with other statistics units of the Government, shall be disseminated to the public on a regular basis. The policy also states that, in addition to the summary or aggregate statistics derived from the surveys, census microdata will also be disseminated (however, in practice, the microdata cannot be freely downloaded; the procedure that has to be followed to access microdata is explained below). Metadata relating to these microdata shall also be provided to help researchers understand what the data are measuring and how they have been created.

The policy does not appear to have been updated since 2014.

The policy defines microdata as data collected on an individual object, the statistical unit. Units of observation can be households, individuals, agricultural holdings, etc. The policy defines two types of microdata files and explains the procedures that must be followed if requesting the release of microdata.

Extract from policy document

Types of micro data

---

50 "Department of Census and Statistics."
51 "Department of Census and Statistics."
52 "Lanka Datta."
53 "Department of Census and Statistics."
54 Dissemination Policy on Microdata Department.

• Public Use Files (PUFs): Microdata files that are disseminated for general public use outside DCS. They have been highly anonymized by removing names and addresses and by suppressing/ collapsing geographic and respondent characteristic details to ensure that identification of individuals is highly unlikely. These files are made available for downloading from the DCS site to individuals who identify themselves by name, provide their email addresses, and agree to abide by the terms and conditions appropriate for a PUF. (Conditions include the following; that the data will not be redistributed or sold to other individuals, institutions, or organizations without the written agreement of the DCS, that the data will only be used for statistical and scientific research purposes, etc.)

Licensed files: These files require that there be a signed agreement between the DCS and major users, to permit them to access data files that are more sensitive than PUFs e.g. datasets which make available geographic variables beyond the domain level or full details of some indirect identifier variables. For these files, all direct identifiers have been removed, and some characteristic details may be collapsed or removed. Licensing agreements are only entered into with bona fide users working for registered organizations. The primary and secondary researchers must be identified by name, and a responsible officer of the organization must endorse/ co-sign the license agreement.

The policy also defines 'authorized users' to whom the microdata can be released. These should be 'specialized users with advanced quantitative skills, such as the following:

- Policymakers and researchers employed by line ministries and planning departments who are engaged in the development of regional and national strategies and programs, including the monitoring and evaluation of these programs.
- International agencies involved in the conduct of special studies aimed at identifying development and support opportunities, and the development programs and infrastructures within DCS
- Research and academic institutes involved in social and economic research
- Students and professors mainly engaged in educational activities, and
- Other users who are involved in conducting scientific research (to be approved on a case-by-case basis).

It can be seen from the above that the process of accessing microdata is not straightforward and is restricted only to certain users.

The policy also lists a website where metadata can be provided to the public; however, the website link could not be accessed at the time of research.[55]

2.3.5 Credit Information Bureau of Sri Lanka (CRIB)

The Credit Information Bureau of Sri Lanka (CRIB) is the first credit bureau in the South Asian region, and was established by the Credit Information Bureau of Sri Lanka Act No. 18 of 1990 (as amended).[56] CRIB is an independent statutory body and a public-private partnership, with the Monetary Board of the Central Bank of Sri Lanka holding much of the equity. The shareholders include all licensed public and private Commercial banks, specialized banks, finance companies, leasing companies, and other designated member

[55] "Dissemination Channel Metadata for DCS studies are provided to public through the DCS NADA http://statistics.sltidc.lk/index.php/home."

[56] Credit Information Bureau of Sri Lanka Act No: 18 of 1990.

institutions. It is trite to note that when it was first established in 1990, it was the first of its kind in South Asia. The CRIB collects, collates, and disseminates credit information for all borrowers and prospective borrowers. Credit information is made available to licensed financial institutions, the Central Bank of Sri Lanka, and other entities that have been approved by the Monetary Board (Section 7B). Additionally, a person can request their report by following the procedure mentioned.[57]

2.3.6 Declaration of Assets and Liabilities

The Anti-Corruption Act, 2023, is significant not only for the powers vested in the Bribery Commission but also for establishing a process for citizens to access the assets and liability details of public officials. It was enacted to help Sri Lanka rank higher in global transparency and ease of doing business indices.[58] Section 88 states that the public can access the electronic centralized system through the official website.[59] Personal details such as residential address, bank account details, date of birth/passport number of individuals, etc., are redacted. Previously, the Declaration of Assets and Liabilities Act Law No. 1 of 1975 provided for disclosure but mandated that such information be kept confidential.

2.4 Policies/ Strategies/Standards relevant to increasing access to data in Sri Lanka

Sri Lanka has introduced several policies and strategies to support its vision of a robust data governance framework, particularly under the purview of the Ministry of Technology, Digital Government, and Digital Economy. These initiatives aim to modernize governance, enhance digital services, and foster economic growth through technology. However, significant challenges remain, including concerns about institutional capacity, the availability of training, and the practical implementation of these policies. These issues could hinder the country's ability to realize the potential of its digital transformation efforts fully.

This section outlines some of the key policies and strategies relevant to data governance in Sri Lanka.

2.4.1 Digital Government

Digital Government Strategy 2020-2024

The key strategies are:

1. Citizen and business-focused solutions - A user-centric approach to be adopted to design, develop, and integrate services, catering to the requirements of citizens and businesses.
2. Shared digital services and platforms- The new digital services that will be common, interoperable, and user-friendly platforms with the aim of reducing the >

[57] "CRIB Score Reports - Individual | Credit Information Bureau of Sri Lanka."
[58] "Sri Lanka Leader to Appoints Panel to Amend Flaws Anti-Corruption Law."
[59] Anti Corruption Act 2023.

time and effort. Data standards would also be set, and a data architecture developed to ensure the usability of data across Government digital platforms and services.

3. Develop high available and secure systems - Systems to be designed, developed and operated in a manner that will be resilient to cyber threats, in order to > protect citizens, business and government data stored and shared across systems.
4. Unified approach towards Digital Transformation- Processes to be reengineered and digital technology to be applied in integrating business requirements, policy, operations and technology communities, in order to transform public services.

The Digital Government architecture, as given in the Strategy, has been extracted in Figure 2 below.

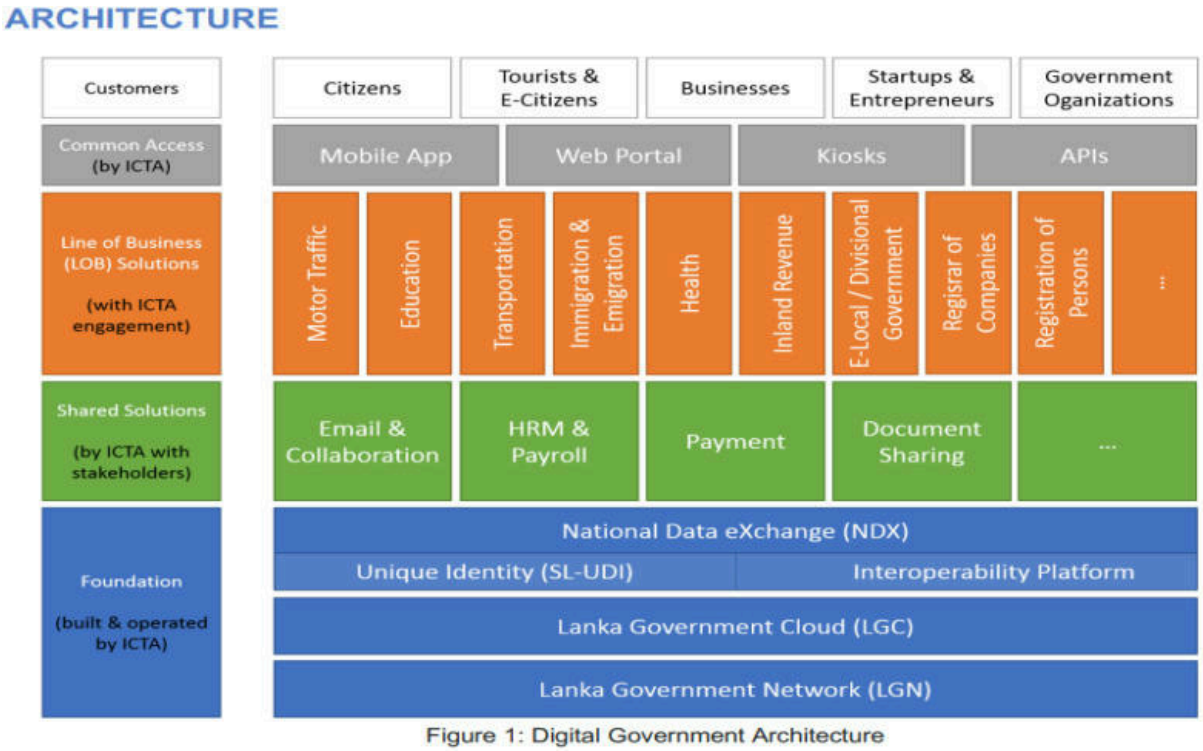

Figure 2: Digital Government Architecture

Source: Digital Government Strategy 2020-2024

National Digital Government and Governance Policy (Draft)

The policy directs the government to achieve results whilst building connected communities with the use of technology and introduces the six (6) principles of citizen convenience; citizen participation; citizens' rights; cost saving; transparency; innovation and transformation.

The policy is still in its draft stage.[60] The draft that is made available says explicitly, "Please do not quote."

The Digital Government Policy ambitions have been linked to "Associating Good Governance Principles Council of Europe ELoGE model."[61]

---

60 National Digital Government/Governance Policy for Sri Lanka.

61 Good Governance, "12 Principles of Good Governance - Good Governance - Www.coe.int."

The detailed policy objectives and various other draft policies under the "Digital Government" initiative are in the Annexure.

Observations

The policies, as detailed in the Annexure, are all in draft form; hence, their inconsistencies should be viewed with some latitude. However, it is essential to note that several of these policies have been stuck in the development stage for years. The "National Data Sharing Policy," for example, has been in draft form since 2013.

The "Information Classification Framework" that is meant to provide guidance to PAs regarding disclosure under RTI has *inter alia* classified "salaries" and "personal case files such as benefits, program files or personnel files" as "Confidential" information. Confidential information is said to refer to that "when compromised, may lead to a high probability of causing damage to *national security, internal stability, national infrastructure, forces, commercial entities or members of the public*". This is directly in conflict with the RTI Act and the Orders of the RTI Commission. The RTI Commission has, time and again, ordered disclosure of salary details and details of benefits / allowances paid to public officials.[62]

There are also privacy implications associated with these initiatives that warrant attention.

Open Standards / Interoperability Projects

It is noteworthy that several standards have been implemented under the "Digital Government" pillar. These play a crucial role in the overall data governance structure.

Sri Lanka Government Enterprise Architecture (SL-GEA) is the whole of government architectural approach for a digitally inclusive Sri Lanka.[63] A first draft version (v 1.0) was released in April 2023.

1. SL-UDI (Sri Lanka Unique Digital Identify) (Ongoing- Not yet completed)
2. Lanka Interoperability Framework (LIFe) – life.gov.lk (explained in Annexure) ICTA initiated the standardization process in collaboration with governmental custodians of several data domains to ensure interoperability in government information systems. One example is the standardized location codes for administration zones defined by the Ministry in charge of Home Affairs (http://moha.gov.lk:8090/lifecode/home).

   LIFe will make way for National Data Exchange (NDX) (Ongoing, not yet completed). The National Data Exchange will be the central repository for all government information, and even those belonging to another department can be accessed.
3. Lanka Government Network (LGN) (explained in Annexure)
4. Lanka Government Cloud (LGC) (explained in Annexure)
5. Lanka Government Payment Service (LGPS) - to process electronic payments
6. GovSMS Portal
7. Government Single Window Portal - gov.lk

---

62 "Table of RTIC Decisions."

63 Information and Communication Technology of Sri Lanka (ICTA), *Sri Lanka Government Enterprise Architecture: The Whole of Government Approach.*

8. Open Data Portal – data.gov.lk

   The Open Data Portal has been designed to disseminate data from government back-ends to citizens, businesses, and all the other relevant stakeholders. The Open Data initiative of the Government of Sri Lanka makes several datasets freely available to the public through this web page. The open data page focuses on machine-readable (i.e., well-structured and open) datasets. It is noted that there are only a few data sets. Agriculture has 45, the largest number of datasets. Travel and tourism each have one. The datasets are also not being updated regularly: as of December 2024 the latest dataset is from 2022.[64] It was noted that in March 2025, one dataset from 2024-2025 was made available.

9. Government Information Center (GIC) – gic.gov.lk – for citizen services to provide service-related information in two national languages and in English to the public via interoperable cloud services, supporting collaboration and integrated government service, along with a central call center outsourced to a private operator.

10. National Spatial Data Infrastructure (NSDI) – nsdi.gov.lk – It enables spatial data standardization; avoiding data duplication, improving data quality as well as transparency in data sharing across government organizations, and providing a technological platform for developing spatial data decision support tools.

11. LankaPay LankaSign - Government entities that introduce 'Digital Signature' for adoption at their organization are required to obtain services from a 'Certificate Service Provider (CeSP)'. Currently, the only CeSP authorized in Sri Lanka is LankaPay (Pvt) Ltd (under the brand name LankaSign) established by the CBSL and other licensed commercial banks.[65] LankaSign uses X.509 digital certificates and associated technologies.

In addition to these standards in the Digital Government, there is a draft policy on Sri Lanka's FOSS Adoption.[66] It states that most of the government's projects have been developed using FOSS. It mentions that using free and open source software has been the practice but makes no mention of preferring FOSS for projects. It can be gathered that FOSS has been the preference.

Birth, Marriage, and Death Certificates Digitalization and Sharing Project

In November 2024, the government announced a new initiative to issue copies of birth, marriage, and death certificates to Sri Lankans living abroad through Sri Lankan embassies, to provide greater convenience for those living abroad.[67]

The program will be launched as a pilot project across seven selected foreign missions, including embassies in Kuwait, Japan, and Qatar, as well as consulates in Melbourne (Australia), Toronto (Canada), Milan (Italy), and Dubai (UAE).[68]

---

64 "Open Data Portal - Sri Lanka."

65 "LankaSign Certification Service Provider (CSP) | Knowledge Center - Lanka Clear."

66 Information and Communication Technology of Sri Lanka (ICTA), "Sri Lanka Government FOSS Adoption Draft."

67 Presidential Secretariat, "A Strategic Approach to Digitize Government Services."

68 Presidential Secretariat.

The press release states that efforts are underway to enhance the e-BMD (electronic Birth, Marriage, and Death) database system in Sri Lanka, which is jointly managed by the Registrar General's Department and the Ministry of Foreign Affairs. This would allow birth, marriage, and death certificates to be issued through foreign embassies, following a model already in place for obtaining certificates at Divisional Secretariat offices across Sri Lanka.[69]

Electronic Vehicle Revenue License Project

There is currently an online system for the e-Vehicle Revenue License. However, it has been plagued by several issues, including slow processing and limited capacity. An update is now being planned through which vehicle owners will have the convenience of obtaining their revenue licenses from any Province, irrespective of the vehicle's original registration province.[70]

Mandatory Integration Standard for National Quick Response (QR) Codes

Through Payments and Settlements Systems Circular No. 13 of 2020 dated 14 May 2020 ("QR Code Circular 2020"), all licensed Banks and licensed Operators of Mobile Phone-based e-money systems who offer QR Code-based payment solutions were mandated to join LANKAQR.[71] It can be noted from an earlier circular that the LANKAQR code standard is based on the EMV QR Code, a proprietary, widely-used specification.[72] By mandating a common standard, the system reduces fragmentation and vendor lock-in, thereby promoting openness in data governance through standardized data flows, enhanced transparency, and a more inclusive digital payment ecosystem.

Digitizing Registration of Persons (Digital ID)

The project to digitize the existing national digital ID (e-NIC) has been underway since 2011. Inquiries with industry insiders revealed that the Department of Registration of Persons (DRP) shares selected details from a database of national identity cards (NIC) with certain public and private entities to verify the authenticity of data submitted through an API system. For example, with a digital payments solution partner (a banking or non-banking financial institution or licensed operator), the DRP may authenticate the NIC details they have received.

The e-NIC project has now paved the way for a unique digital ID, which would integrate the e-NIC within it. Instead of using proprietary platforms, the government has decided to use open-source MOSIP for this project.[73] There have been concerns surrounding the capture of data and the use of the platform in collaboration with an Indian counterpart.[74] In response, it has been stated that "A certified Indian system integrator will customize MOSIP for Sri Lanka, while local IT professionals will be trained for full operation, maintenance, and the future development of the system."[75]

Cloud Strategy and Cloud Policy (Draft)

---

69 Presidential Secretariat.
70 "Online Registered Vehicle Information Service - Department of Motor Traffic - Sri Lanka."
71 "Payment and Settlement Systems."
72 "Payment and Settlement Systems Circular No 6."
73 "Digital ID Launch by 2026: A Big Step Toward a Modern Sri Lanka."
74 Weerasinghe, "The New Digital ID to Be an Integrated e-NIC/MOSIP Solution."
75 "Digital ID Launch by 2026: A Big Step Toward a Modern Sri Lanka."

In June 2025, two drafts, titled "Towards a Sovereign Cloud Strategy for Sri Lanka" (Version 0.4) ("Cloud Strategy") and "Draft Revised Cloud Policy and Procurement Guidelines for Interim Use" (Version 0.2) ("Cloud Policy"), were released for public consultation.[76] The Cloud Strategy, *inter alia*, highlighted the need for a "hybrid and collaborative model" as opposed to an "exclusively government-owned and locally managed data centers." Particularly, one of the objectives is to ensure that "data, especially public sector and critical sector data, is stored, processed, and governed within Sri Lankan legal jurisdiction in alignment with emerging national data protection regulation and regulatory frameworks". The Cloud Strategy operationalizes data sovereignty, classification, oversight, and compliance in the cloud environment. It highlights tensions and trade-offs: e.g., between openness to hyperscalers vs. sovereignty; innovation vs. strict localization; fragmented oversight vs. centralized regulation. International case studies from GAIA-X (France and Germany), India, Singapore, UAE are also discussed.[77]

The Cloud Policy mandates a classification system for government data (public, internal, confidential, restricted, top secret) and ties these categories to deployment models and sovereignty requirements. A four-tier sensitivity model ensures that the most critical workloads (e.g., national security, top secret data) are hosted in Digital Sovereignty Zones ("DSZ") within Sri Lanka, under exclusive legal and operational control. DSZ are defined as "secure, government-certified hosting environments physically located within Sri Lanka that operate entirely under Sri Lankan jurisdiction."[78] They are designed to host the country's most sensitive digital assets, including top secret and national security-related data. Procurement is treated as a core governance instrument: all cloud procurements must align with the data classification and sovereignty tiers; preference is given to providers compliant with Sri Lankan law and capable of supporting sovereign control and integration with local/sovereign cloud infrastructure; procurement processes must promote competition, innovation and value for money; contracts are required to include data residency, portability, service continuity, auditability and exit mechanisms; strategic partnerships (e.g., hyperscalers) require prior technical and legal review by designated authorities; procurements must provide for future migration to national sovereign cloud through modular designs and flexible contract terms; and systems at sensitivity Levels 2 (federated or hybrid cloud) and 3 (high sovereignty + conditional localization) must support hybrid operation and interoperability while maintaining classification and sovereignty compliance.[79]

In summary, the procurement policy is being used proactively to enforce sovereignty, portability and auditability — making contract design and enforcement a central research focus. The policy explicitly targets vendor-lock-in through contractual safeguards and cross-border risks via hybrid/interoperable requirements and migration readiness, raising questions about technical feasibility and costs. To implement these requirements, institutional capacity for technical/legal reviews, monitoring, and DSZ certification remains critical.

Unified digital payments – GovPay

---

76 ICTA, "Public Consultation: Call for Views on Cloud Policy and Strategy for Sri Lanka."

77 Karunasena et al., *Towards a Sovereign Cloud Strategy for Sri Lanka: A Government-Regulated, Private-Sector-Driven Approach to Enable Local Innovation and Trusted International Collaboration.*

78 "Draft Revised Cloud Policy and Procurement Guidelines for Interim Use."

79 "Draft Revised Cloud Policy and Procurement Guidelines for Interim Use."

GovPay is an online payment platform designed to facilitate digital transactions for government services.[80] It enables citizens and businesses to make payments for various government-related transactions, including taxes, fines, utility bills, and educational fees, through banks and digital wallets. The initiative is to streamline financial transactions within government institutions. Importantly, traffic fines can also be paid using the app.[81] However, user experiences have indicated shortcomings in implementation.[82]

2.4.2 Digital Economy

Since its early days, ICTA has been involved in various initiatives to encourage the digitization of multiple initiatives. The e-Sri Lanka initiative, launched in 2002, aimed to utilize ICT to foster economic growth, reduce poverty, and enhance the quality of life. This initiative marked Sri Lanka's entry into the digital economy, with a focus on e-governance, rural ICT infrastructure, and capacity building.

Connected Government

According to ICTA, "connected government" refers to a seamless integration of information, communication, and technology systems across various government entities, enabling efficient data sharing, collaboration, and service delivery.The National Digital Economy is one of the initiatives towards "connected government."[83] The other relevant policies/recommendations include the Sri Lanka Government Enterprise Architecture V1.0, an integrated CB approach for government digital transformation, a digital maturity model for GoSL, digital transformation units, a chief digital information officer, a digital government competency framework, and use cases for connected government.[84]

National Digital Economy Strategy 2023-2030

The 2023-2030 strategy was being developed when this research was carried out. The strategy is stated to, *inter alia,* focus on "reducing barriers to accessing digital technologies and utilizing digital tools to expand access to markets, employment, and educational opportunities for all."[85] Notably, the new strategy invited comments from the general public through a questionnaire.[86]

The figure below has been included in the questionnaire to give the public an understanding of the proposed strategy.[87] It is encouraging to note that "legal and regulatory framework" and "data governance" have been included as key enablers. Figure 3 below illustrates the strategy.

80 GovPay, "Secure & Convenient Payments."
81 GovPay, "Pay Traffic Fines Online with GovPay."
82 Hassim, "My First Experience with GovPay."
83 "Information and Communication Technology Agency of Sri Lanka."
84 "Information and Communication Technology Agency of Sri Lanka."
85 "Invitation to Provide Input on National Digital Economy Strategy | Ministry of Technology."
86 Google Docs, "Stakeholder Consultation on Sri Lanka's National Digital Economy Strategy."
87 Google Docs, "Stakeholder Consultation on Sri Lanka's National Digital Economy Strategy."

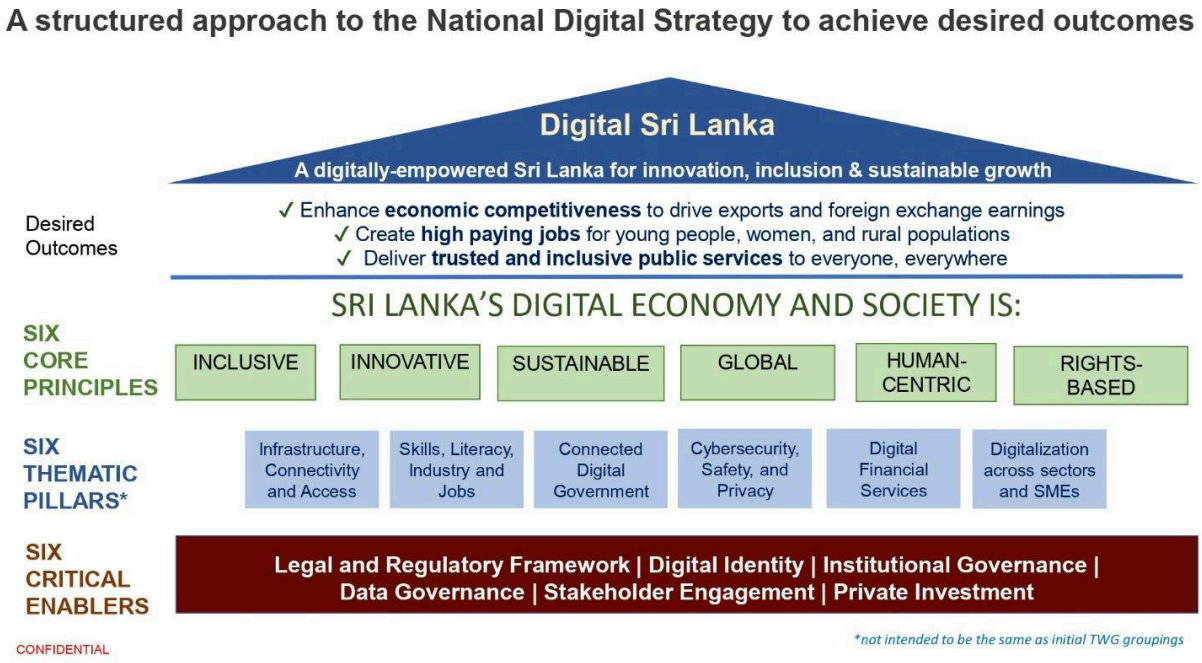

Figure 3: National Digital Economy Strategy

Source: National Digital Economy Strategy 2023-2030

Observations

The current strategy is certainly more elaborate and includes a focus that is much more comprehensive. If they can be implemented into workable outcomes, it would be commendable.

Data for Public Good - National Fuel Pass (NFP)

In July 2022, to address the issue of acute fuel shortage, the NFP was launched. At the time of its launch, the Ministry of Power and Energy stated that "National Fuel Pass" was a convenient and easily accessible solution for the public to obtain fuel, facilitating an allocation-based fuel distribution method. It is a stellar example of utilizing data for the public good. The primary objective of the NFP was to ensure equitable access to fuel for all Sri Lankans. By requiring vehicle owners to register for a weekly fuel pass, i.e., a weekly allocation of fuel, there was also the possibility of monitoring hoarding.[88] The NEP, an initiative by the ICTA and two private entities, was implemented nationwide.[89]

The existing digital infrastructure maintained by the Department of Motor Traffic was critical for the implementation of the NFP, as it provided an online registered vehicle information service. This database included critical details such as the name, address, and vehicle information of owners.[90] While comprehensive owner and vehicle details can be accessed for a fee, limited information is available free of charge.[91] The success of this should also be attributed to the project's fast and efficient implementation, which avoided the usual procurement procedure delays.[92]

88 "Information and Communication Technology Agency of Sri Lanka."
89 Dialog Axiata PLC, "Dialog Axiata, MIT and ICTA Recognised by the Ministry of Power…."
90 "Online Registered Vehicle Information Service - Department of Motor Traffic - Sri Lanka."
91 "Online Registered Vehicle Information Service - Department of Motor Traffic - Sri Lanka."
92 Samarajiva, *Digitalisation Will Fail, Unless | Daily FT.*

National AI Strategy

The Strategy places emphasis on data governance, committing to the development of a comprehensive data strategy and governance framework to boost the availability, integrity, quality, and protection of AI-ready data assets.[93] It proposes the creation of data-sharing mechanisms, expansion and revitalization of open data platforms, and the establishment of clear guidelines for data management and protection — all designed to underpin evidence-based policymaking, support the private sector. Furthermore, the Strategy calls for a detailed data governance and stewardship framework, including the implementation of processes, policies, regulations, and standards to promote ethical data use and ensure its secure utilization across sectors. It is relevant to note that the AI white paper emphasized a federated data management model, enabling efficient use of high-quality datasets across initiatives, with dedicated subsets of data formatted for AI use.[94]

2.5 Policies that Decrease Access to Data

It is essential to note that the term "decreasing access to information" in this context is not always used in a negative connotation to suggest that such laws are inherently restrictive or detrimental. Instead, this categorization has been employed to differentiate laws based on their impact on individual access to information /data. For instance, legislation such as the Personal Data Protection Act, or policies on cyber security, while limiting access to certain types of information, are vital for safeguarding personal privacy and ensuring data security. These restrictions often serve legitimate and necessary purposes, and their inclusion under this section does not necessarily imply that such laws are blameworthy or unjustified.

Unlike in the previous section on increasing access, we have grouped some laws under broad headings for brevity and ease of understanding.

2.5.1 Security

General – National Security / Curbing Disinformation

Restriction of access to information on grounds of national security can be found in several laws. The key ones include the Sri Lanka Telecommunications Act No. 25 of 1991 ("SLTA"), Computer Crime Act No. 24 of 2007, International Covenant on Civil and Political Rights Act No. 56 of 2007, the Prevention of Terrorism Act of 1979 and Public Security Ordinance No 25 of 1947 (in the event of an Emergency being declared). Section 3 (1) of the ICCPR gives effect to Article 20 of the ICCPR Convention, and states that 'No person shall propagate war or advocate national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.' However, this section has been used in a problematic manner; perpetrators of hate speech against minority communities are often not prosecuted, and the section has also been misapplied to arrest persons who should not have been prosecuted under the Act.[95]

---

93 "National AI Strategy for Sri Lanka."

94 Committee on Formulating a Strategy for Artificial Intelligence (CFSAI), *Artificial Intelligence in Sri Lanka.*

95 *Mohamed Razik Mohamed Ramzy v. B.M.A.S.K. Senaratne.*

The Online Safety Act No. 9 of 2024 ("OSA"), with its broad provisions, seeks to regulate disinformation online, amongst other kinds of information.[96] The Online Safety Act (OSA) has been criticized for laying down broad and vague offences. There is also a lack of clarity in definitions used; the Act centers on the prohibition of 'communication of false statements.' It defines false statements (section 52) ambiguously as "a statement that is known or believed by its maker to be incorrect or untrue and is made especially with intent to deceive or mislead, but does not include a caution, an opinion or imputation made in good faith." The criterion of 'known or believed by its maker to be incorrect' is subjective, and it is unclear how this will be interpreted. A statement is defined as 'any word including abbreviation and initial, number, image (moving or otherwise), sound, symbol, or other representation, or a combination of any of these.'[97]

In November 2024, it was reported that a six-month suspended prison sentence had been imposed on an individual for spreading misleading information about former State Minister Kader Masthan on social media, following a complaint filed under the OSA. This is reportedly the first conviction under the Act. The individual was accused of spreading audio recordings on social media platforms (Facebook and WhatsApp). The judge also ordered the immediate removal of the statements made by the individual on social media about the former State Minister. The judge also ordered the suspect to immediately remove all the statements that he had published on social media about the former State Minister.[98]

Prior to the enactment of the OSA, the SLTA was used to block social media apps and websites to ostensibly curb disinformation. The Telecommunications Regulatory Commission of Sri Lanka has the power to direct licensed telecommunication operators to block access to sites. The SLTA has also been used to restrict access to certain websites, including news websites [[99]].[100]

It should also be mentioned that not only its provisions but also the passage of the OSA has been shrouded in secrecy and riddled with controversies. The introduction of the Online Safety Bill was widely criticized. No stakeholder consultation process was conducted in formulating the Bill, despite many stakeholders calling for widespread consultation. The Bar Association of Sri Lanka called for the Bill to be withdrawn[101]. The procedure for formulating the Bill was not open or transparent; the Asia Internet Coalition (AIC), which represents major tech companies such as Meta, Amazon, raised concerns about the Bill's lack of stakeholder consultation and criticized its potential to suppress dissent and hinder public discourse, potentially hampering the growth of the country's digital economy.[102] The International Commission of Jurists issued a statement noting that the bill would undermine the exercise of human rights and fundamental freedoms in the country, including the rights to freedom of information and expression. The Commission noted that "…Of particular concern are provisions related to the setting up, appointment and functions of an Online Safety Commission and other experts, the vague and over-broad wording of

96 Online Safety Act No 9 of 2024.

97 Online Safety Act No 9 of 2024.

98 *Newswire*, "Online Safety Act."

99 *Raisa Wickrematunga v. Telecommunications Regulatory Commission of Sri Lanka (TRCSL).*

100 Wickrematunge, "Blocked."

101 "BASL CALLS UPON THE GOVERNMENT TO IMMEDIATELY WITHDRAW THE ANTI – TERRORISM BILL ANDTHE ONLINE SAFETY BILL - BASL," accessed October 31, 2023, https://basl.lk/anti-terrorism-bill-and-the-online-safety-bill/.

102 "AIC Warns Sri Lanka's Online Safety Bill Threatens Freedom of Expression."

conduct designated as punishable offences and unnecessary and disproportionate punitive sanctions."[103] The OSA came to be passed notwithstanding all these objections, and notably, the final Act did not include the amendments suggested by the Supreme Court of Sri Lanka.[104]

Proposed amendments to the OSA were published via the Government Gazette in July 2024 (Gazette notification dated 31st July 2024).[105] However, the amendments have not been passed yet at the time of writing. A public call for consultation for amending the OSA was published in August 2025.

A draft cyber security Bill was released in 2023; it was also open for public consultation.[106] The Bbll required accreditation of all cybersecurity service providers. The definition of Critical National Infrastructure was broad, and referred to "the computer, computer program, computer system, or related device identified by the Authority as a Critical National Information Infrastructure under this Act, which is located wholly or partly in Sri Lanka, and its disruption or destruction would create a *serious* impact on the national security, public safety, public health and economic wellbeing of citizens, delivery of essential services or effective functioning of the government or the economy of Sri Lanka." In contrast, the cabinet-approved Information and Cyber Security Policy (detailed below) included a similar definition; but instead of the term "serious" it used "debilitating", which, in our opinion, could be more stringent.

Cyber Security for Government Organisations

Sri Lanka Computer Emergency Readiness Team ("CERT") is the National Centre for Cyber Security, responsible for protecting the nation's cyberspace from cyber threats.[107] At present, there are no requirements to report cyber security incidents to the CERT.

It was established in 2006 as a government-owned private company and functioned as a subsidiary of ICTA until a government policy directive made it independent in 2018. Sri Lanka CERT is a partner of global CERT networks, a member of the FIRST (Forum of Incident Response Teams), Asia Pacific CERT, Cyber4Dev of the European Union, and the World Bank, aiming to build a better cyber security ecosystem for the nation. In September 2025, the National Cyber Security Operations Centre was established to protect the Critical National Infrastructure of Sri Lanka.[108]

National Information and Cyber Security Strategy (Cyber Security Strategy) of Sri Lanka 2019-2023

The Strategy focuses on six strategic thrust areas, detailed in the Annexure.[109]

Achievement of the thrust areas and their progress

We have tracked the progress of the strategy (until Feb 2024).

---

103 "Sri Lanka," "Sri Lanka."

104 Sooriyagoda, "Speaker's Act of Certifying Online Safety Bill Challenged in SC by Sumanthiran."

105 **parliamentofthedemocraticsocialistrepublicofsrilankaOnlineSafetyAmendment2024?**

106 Rajapakse, "Comments on the Cyber Security Bill - Sri Lanka 2023."

107 **srilankacertInformationAndCyberSecurity2023?**

108 "Home | NCOSC."

109 Democratic Socialist Republic of Sri Lanka and Sri Lanka CERT, *Sri Lanka National Information and Cyber Security Strategy 2019-2023.*

The Cyber security Strategy specifically provided for the following:[110]

1. **Digital Infrastructure Protection Agency (DIPA) of Sri Lanka.** The DIPA was to be the apex body for all cyber security affairs in Sri Lanka.

- The DIPA was not established; instead, the recently released Cyber Security Bill provided for the establishment of the Cyber Security Regulatory Authority of Sri Lanka.

2. The table below details progress in terms of **legislation, policies, and standards**.

Table 1: Progress of legislation, policies, and standards

Strategy Objective	Completed or not	Current Status
New Cyber Security Act	Draft is available	Ongoing
Data Protection and Privacy Laws	Act Passed in March 2022	The DPA has been operational since August 2023. The PDPA is not yet in force, save Part V of the Act
Data Sharing Policy for government organizations	An erstwhile Data Sharing Policy drafted in 2013 is available online.	It has not been adopted or implemented.
Baseline information and cyber security standards with the Sri Lanka Standards Institute (SLSI)	No information available publicly.	Both SLSI and CERT are expected to collaborate on this strategy.
Critical Infrastructure Protection Policy	The Cyber Security Bill includes this	Ongoing
Information Security Policy	Policy applicable to Government Organizations has been approved by the cabinet.	Implementation level at government institutions is not known.

3. The third thrust area of "building a competent workforce" has seen limited progress. In reality, there has been a sharp decline in skilled professionals due to emigration resulting from the country's economic and political crisis.

4. Thrust areas 5 (raising public awareness) and 6 (development of public/private partnerships) have seen some progress, but more action is required.

Information Security Policy Framework[111]

Information and Cyber Security Policy ("Information Policy") for the use of government organizations

This cabinet-approved policy[112] took effect in August 2022. This Policy adopts a risk-based approach for implementing an information and cyber security program at the

[110] Democratic Socialist Republic of Sri Lanka and Sri Lanka CERT.
[111] Sri Lanka CERT, "Proposed Information Security Policy Framework for Government Organizations."
[112] **srilankacertInformationAndCyberSecurity2023?**

organizational level. It also provides a set of actions that organizations should implement to identify and protect assets; detect information security incidents in a timely manner; respond to incidents and recover from cyberattacks in an efficient and effective manner. The Policy states that "based on the international standards and best practices such as International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) of the United States of America and has been extensively reviewed by information security experts and senior officers of the government."

Application – All government organizations that are defined as 'Public Authorities' in the Right to Information Act No. 12 of 2016 ("RTI Act") are required to comply with this Policy.

Observations

1. Section 43 of the RTI Act encompasses a broad definition of "public authority" including governmental organizations, private entities that perform public functions, higher educational institutions, including private universities, etc. While the Information Policy is somewhat restrictive, it only mentions "government organizations"; linking it to the RTI Act leads to ambiguity regarding whether it would also apply to other institutions / organizations, such as private organizations included under the relevant provision.
2. The Information Policy has been made effective in August 2022. In December 2023, one year after its operation began, it is unclear to what extent its implementation has progressed.
3. The Information Policy has several compliance requirements, essentially six main policy domains namely, (a) establishment of an information and cyber security governance structure within the organization, (b) identification of assets, asset owners, custodians, and risks, (c) protection of asset, (d) identification of information and cyber security incidents (e) responding to security incidents, and (g) recovery of operations that were disrupted due to an incident.

Complying with these requirements entails a considerable investment of human resources and imposes a significant financial burden. In light of the economic crisis faced by Sri Lanka in 2022, it is unclear how government organizations have implemented this.

Minimum Information Security Standards (Draft v.1)

These standards[113] are said to be based on global standards such as the National Institute of Science and Technology USA, and the International Standards Organization (27002), and global best practices in developing information security standards (e.g., the UK Government's Minimum Cyber Security Standard, Information Security Policy Manual of New Zealand).

The Minimum Information Security Standards provide a risk-based approach to protecting information and IT assets. It requires that a risk assessment be performed on each asset to determine its level of sensitivity and criticality, and to develop appropriate controls to protect it. The "Minimum Information Security Standards" refers to "Classification of Assets" as a mandatory step in assessing the risk associated with information and IT Assets. It states that classification must be in line with the "National Data Sharing Policy" of the Government.

[113] "Minimum Information Security Standards."

Minimum Information Security Standards are developed based on the following six (06) Information Security Principles. (a). Information Security Governance -This specifies the strategic alignment and accountability framework that provides insight to ensure that information security activities are properly managed within the organization. (b). Identify- This identifies the organization's assets (information and IT assets), and the risks associated with those assets. (c). Protect-This outlines the controls that shall be implemented to prevent, limit or contain the impact of a potential information security event or incident. (d). Detect- This outlines the activities that shall be carried out to discover information security events in a timely manner. (e. Respond- Provides guidance on activities related to planning and testing responses to cyber security incidents, and to initiate these in case of a cyber-attack. (f). Recovery: Provide guidance on activities that shall be carried out to resume normal operations after a cyber security incident or disaster.

Observations

While Sri Lanka has made significant efforts to develop information and cyber security frameworks — including the 2019–2023 Cyber Security Strategy, the Information and Cyber Security Policy for Government Organizations (2022), the Draft Minimum Information Security Standards, and related legislative initiatives such as the Personal Data Protection Act No. 9 of 2022 — the current policy landscape reflects fragmentation, duplication, and lack of harmonization, especially when viewed through the lens of data governance.

This multiplicity of overlapping frameworks has several implications for the governance, protection, and management of data in Sri Lanka:

1. Lack of Policy Coherence Undermines Data Governance

   Multiple frameworks impose parallel obligations without a unified architecture. For example, while the PDPA mandates the appointment of a Data Protection Officer, the Information Security Policy requires the appointment of Information Security Officers and the establishment of Information Security Committees. These roles are distinct but potentially overlapping in terms of data classification, breach response, and risk assessment — leading to confusion, inefficiencies, and duplication of effort at the institutional level. In a resource-constrained context, this hampers effective governance of both personal and institutional data.

2. Unclear Applicability Creates Gaps in Data Accountability

   The Information Security Policy applies to entities defined as "public authorities" under the RTI Act. However, the RTI Act's definition of public authority is expansive and includes certain private entities and educational institutions. The Policy's selective reference to only "government organizations" creates ambiguity about the applicability of information security responsibilities to data-holding institutions outside the traditional government sector — such as public–private partnerships, state universities, and non-state actors performing public functions. This vagueness risks creating grey areas in data security accountability.

3. Absence of Interoperability Between Frameworks Weakens Trust in Data Handling

   The draft Minimum Information Security Standards references the National Data Sharing Policy as essential to risk-based classification of assets — yet this 2013 policy remains unadopted and unimplemented. This creates a vacuum in how sensitive or

critical data should be classified and shared across government departments or with external actors.

4. Operational Gaps in Implementation

   While policies exist on paper, actual implementation remains unclear. There is little publicly available information on how far the Information Policy has been adopted across institutions, or whether government organizations have the human, financial, or technical capacity to operationalize its six policy domains (e.g., asset identification, incident response, recovery). This disconnect between policy and practice undermines the security of critical data systems and exposes the state to systemic data vulnerabilities, especially in times of crisis.

Financial Sector

A plethora of sector-specific concerns may arise in data governance requirements. We specifically focus here on the financial sector due to the existing requirements for data storage and potential conflicts with the PDPA.

Central Bank of Sri Lanka ("CBSL")- Banks and Non-Banking Financial Sector

The Regulatory Framework on Technology Risk Management and Resilience for Licensed Banks, Banking Direction No 16 of 2021 (applicable to licensed Banks) ("Banking Direction on Technology Risk") and the corresponding Technology Risk Management and Resilience Finance Business Direction No 1 of 2022 (applicable to licensed financial companies) provide for compliance requirements concerning the data of financial institutions [[114]].[115] We have limited our analysis below to the Banking Direction on Technology Risk, as the corresponding non-banking directions are similar or less stringent.

The Licensed Banks should have in place 'Critical Information' ("CI") systems. According to the Banking Direction on Technology Risk, amongst others, systems used for Know Your Customer (KYC) are a part of the CI system. For those designated as CI systems, and the relevant licensed bank has been identified as a Domestic Systemically Important Bank, a Disaster Recovery arrangement has to be located locally.[116]

Where an information system infrastructure is managed or owned by third-party service providers, such as cloud servers located outside Sri Lanka, the Banking Direction on Technology Risk states that it must only be in locations approved by the licensed Bank's Board of Directors.

The Board's approval is necessary regarding the adequacy and effectiveness of the legal and regulatory environment in such locations to protect the interests of the Licensed Bank, its customers, the CBSL, and the Sri Lankan judiciary.[117] It can be gathered that CBSL has included these provisions under the Direction as a means of protecting Sri Lankan residents' data from being utilized/taken over by foreign jurisdictions on the basis of data sovereignty.

---

114 Banking Act Directions.

115 "Finance Business Act Direction No 1 of 2022."

116 Banking Act Directions.

117 Banking Act Directions.

Of particular relevance is that the Direction mandates that Licensed Banks must ensure that specific contractual clauses are included in agreements with third-party service providers.

1. If customer data is being exposed to third-party service providers, the CBSL and its officers should be given rights to examine/audit such activities, similar to a situation where such activities were being conducted internally in the Licensed Bank.
2. The third-party service provider must provide information as may be requested by the Director of Bank Supervision concerning the services provided to the Licensed Bank;
3. The rights of the Sri Lankan judiciary to request and obtain any information or data relating to the services provided to the Licensed Bank either directly or through the Licensed Bank;
4. Third-party service providers must facilitate internal auditing requirements and information security testing requirements, including red team exercises

Overall observations

In most instances, the third-party service providers, particularly those located outside Sri Lanka, use standard contract terms. Licensed banks or non-banking financial institutions are not in a position to negotiate or vary these terms, as cloud service providers use their standard templates. This practical difficulty has been observed. Additionally, the implications of requiring contractual terms as aforementioned could result in banks losing out on such services or being unable to comply with the Direction. Under Section 26 of the Personal Data Protection Act No. 9 of 2022, cross-border data transfers are permitted for entities that meet certain contractual obligations as stipulated by the Data Protection Authority.[118] However, under the said Banking Direction on Technology Risk, the CBSL should be given the right to examine/audit customer data. Similarly, the rights of the Sri Lankan judiciary to obtain information as needed should also be guaranteed through contractual safeguards. These requirements not only go beyond those of the Personal Data Protection Act but are also restrictive to the cross-border processing of data.

2.5.2 Privacy / Data Protection

Personal Data Protection Act No 9 of 2022 ("PDPA")

The PDPA was passed in Parliament (and certified by the Speaker of the House on 19th March 2022).[119] Part V of the PDPA, which deals with the establishment of a Data Protection Authority ("DPA"), came into operation in July 2023. The Board of Directors under the PDPA has been appointed by the President, subsequent to an Order issued by the Minister, as per Gazette Notification 2341/59 dated 21st July 2024.[120] Another gazette notification, No. 2366/08 dated 08th January 2024, containing a similar Order, states that the PDPA will come into operation on 18th March 2025.[121] In March 2025, the PDPA Amendment Bill was gazetted. As of this date, the amendments have not yet been passed.

The PDPA is the only comprehensive data protection legislation in Sri Lanka governing the collection, use, storage, and disclosure of individuals' personal data. The PDPA applies to all

118 **srilankaPersonalDataProtection2022?**
119 **srilankaPersonalDataProtection2022?**
120 *Personal Data Protection Authority progresses with Board appointment | Daily FT.*
121 Gazette on Operation of Personal Data Protection.

data controllers (public and private) in respect of the personal data of individuals that they collect, use, store, disclose, etc. (collectively "**processing**"). The PDPA closely follows the GDPR model in several respects, including legal bases for processing, cross-border data transfers subject to an adequacy decision for public authorities (proposed amendments have removed the requirement for an adequacy decision), amongst others. The PDPA is discussed in detail in the next section, i.e., Part B.

2.5.3 Intellectual Property

Intellectual Property Rights Act, 2003

The Intellectual Property Rights Act, No. 36 of 2003 governs copyrights and related rights; industrial designs; patents, trademarks and service marks; trade names; layout designs of integrated circuits; geographical indications; unfair competition and undisclosed information (e.g., trade secrets).[122] All trademarks, designs, industrial designs, and patents must be registered with the Director General of Intellectual Property. However, no legal provisions currently exist for registration of trade secrets.

The works protected under the Act are listed in Section 6, which includes *computer programs* (Section 6(a)). Databases are protected as *derivative works* under Section 7(b) — this covers collections of works or data (including databases), whether in machine-readable or other forms, as long as the selection, coordination, or arrangement of their contents is original

Section 11 of the Act, on fair use, recognizes exceptions for research purposes. The section specifies that the fair use of a work (including reproduction of a work), for research purposes, is not an infringement of copyright. In order to decide whether a case falls within the definition of 'fair use,' several factors are considered including whether the work is being used for commercial or non-profit educational purposes, the portion of the work used in relation to the whole copyrighted work, and the effect of the use on the potential market value of the work.[123]

The National Intellectual Property Office (NIPO) of Sri Lanka, established under the Intellectual Property Act No. 36 of 2003, is mandated with the administration of the intellectual Property System in Sri Lanka. Sri Lanka is a WTO member and a party to the Paris and Berne Conventions, the Patent Cooperation Treaty (PCT), and Trademark Law Treaty (TLT), as well as the Marrakesh VIP Treaty.[124]

With regard to data governance, it should be noted that the Intellectual Property Rights Act of Sri Lanka does not contain provisions for transient or incidental storage of a work or performance for the process of electronic transmission or communication to the public. It does not, for example, have any provisions similar to the amendments that were introduced in 2012 to the Indian Copyright Act, which provide for '…the transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public' and '…transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration[125] .[126] The

---

122 Intellectual Property Act.

123 See Section 11.

124 "Paris Convention for the Protection of Industrial Property."

125 The Copyright (Amendment) Act.

126 **CopyrightAct1957a?**

lack of such amendments means that there are no provisions under Sri Lankan law to legalize the transient/incidental storage of works carried out by search engines such as Google.

AI authorship

Sri Lanka's copyright law does not mention copyright for works purely generated by AI.

The Act defines the author of a work as 'the physical person who has created the work' (Section 5). There is no mention of how the authorship of any original literary, artistic, or scientific work that is computer-generated would be decided.

Section 6 of the Act specifies different categories of works that shall be protected, and this includes computer programs. The section states, 'the following works shall be protected as literary, artistic or scientific work (hereinafter referred to as "works") which are original intellectual creations in the literary, artistic and scientific domain, including and in particular (a) Books, pamphlets, articles, computer programs and other writings. "Computer program" is defined as '…a set of instructions expressed in words, codes, schemes or in any other form, which is capable, when incorporated in a medium that the computer can read, of causing a computer to perform or achieve a particular task or result.'

This indicates that while computer programs (software) themselves are protected by copyright, literary and artistic works that are computer-generated are not covered.

It is interesting to note that the white paper on AI Strategy for Sri Lanka mentions that there are different approaches to the use of copyrighted works, including the approach in Japan, where copyrighted works can be used in foundational models, and they should be considered.[127]

Observations

While the overall IP ecosystem in Sri Lanka has improved in recent years, the country lacks an effective strategic policy and coordination among entities involved in the implementation and execution of laws. This has led to counterfeit products being freely available in Sri Lanka.

The lack of adequate IPR protection has been criticized by local agents of international companies representing the recording, software, movie, clothing, and consumer products industries on the basis that this damages their business interests in Sri Lanka.

In recent years, legal challenges have arisen in other jurisdictions over datasets that include copyrighted materials allegedly being used without consent to train AI models. In Sri Lanka, such legal cases have not yet arisen. But in the future, legal challenges may be posed, for example, with regard to the use of copyrighted Sinhala language material to train AI models. (Under the Sri Lankan Intellectual Property Rights Act, an author's copyright is protected during the lifetime of the author and for a further period of 70 years from the date of the author's death.) It remains to be seen how such legal challenges will be decided, for example whether Section 11 of the Intellectual Property Rights Act (on fair use) could be used to justify the use of such materials. The section specifies that the fair use of a work (including reproduction of a work), for research purposes, is not an infringement of

[127] Committee on Formulating a Strategy for Artificial Intelligence (CFSAI), *Artificial Intelligence in Sri Lanka.*

copyright. In order to decide whether a case falls within the definition of 'fair use,' several factors are considered including whether the work is being used for commercial or non-profit educational purposes, the portion of the work used in relation to the whole copyrighted work, and the effect of the use on the potential market value of the work.

2.5.4 Trade agreements

Sri Lanka has signed free trade agreements (FTAs) with India, Pakistan, Singapore, Thailand and is currently negotiating an FTA with the PRC. The FTAs with India and Pakistan cover only trade in goods.[128]

FTA with Singapore[129]

This FTA came into force on May 1, 2018. It covers: investment, goods, services, trade facilitation, government procurement, telecommunications, e-commerce, and dispute settlement. Article 9.5 requires that both Sri Lanka and Singapore maintain domestic legal frameworks consistent with UN ECC.[130] The 2017 ETA amendment aimed to strengthen existing provisions by transitioning government transactions to the digital era through the use of stronger and more secure electronic-based authentication methods for all categories of Government transactions, including electronic tax filings, e-procurement, and other revenue-based transactions. The amendment also facilitates the electronic filing of any application, petition, plaint, answer, written submission, or any other document in any Court. This would enhance the ability to adopt e-filing in original Courts, which the Supreme Court and Appellate Procedure Rules do not govern.

The Electronic Transaction (e-Registration of Persons) Regulations No. 1 of 2019, authorizes and facilitates the use of electronic documents and electronic records by the Commissioner-General under the Registration of Persons Act, No. 32 of 1968.[131] A circular in 2021 reiterated the need for government institutions to use electronic records under the ETA.[132]

Cross-border data flows

Chapter 9 deals with electronic commerce. There are also provisions on personal data protection. Article 9.9 deals with cross border transfer of information by electronic means. The said article states that both countries may have their own regulatory mechanisms for cross-border data transfer. However, "flow the cross-border transfer of information by electronic means, including personal information, *when this activity is for the conduct of the business of a covered person*" should be allowed. A "covered person" means an investor or investment (excluding one in financial services) or a service supplier, excluding financial services. There can be a derogation on this free cross-border flow, provided it is to achieve a legitimate public policy objective.

Mutual cooperation

Article 9.12 calls for mutual cooperation, *inter alia*, in exchange for information and sharing experiences on "regulations, policies, enforcement and compliance regarding electronic

---

128 Department of Commerce, USA, "Sri Lanka Country Commercial Guide."

129 **republicofsingaporeSriLankaSingapore2018?**

130 **republicofsingaporeSriLankaSingapore2018?**

131 Electronic Transaction (e-Registration of Persons) Regulations No. 1 of 2019.

132 Presidential Secretariat, Sri Lanka, "Use of Electronic Documents and Electronic Communication for Official Use."

commerce, including: (i) personal information protection; (ii) security in electronic communications; (iii) authentication; and (iv) e-Government."[133]

Observations

Little information is made available in the public domain regarding the cooperation that has actually taken place or whether any enforcement actions have been initiated since.

Regional Agreements

Sri Lanka is a member of the South Asian Association for Regional Cooperation (SAARC), the South Asian Free Trade Area (SAFTA), and the Asia-Pacific Trade Agreement (APTA). However, these do not appear to relate to data governance.[134]

Crimes and Reporting

Sri Lanka became a signatory to the Convention on Cybercrime (ETS No. 185, "Budapest Convention") in 2015 and signed the second additional protocol on Enhanced Co-operation and Disclosure of Electronic Evidence in November 2022. The Mutual Assistance in Criminal Matters Act No. 25 of 2002 was amended in 2018 to ensure compliance with the Budapest Convention.[135] It provides for, among other provisions, expedited preservation of computer data: "the expedited preservation of stored computer data and expedited disclosure of preserved traffic data and data retention."[136]

Where there are financial transactions of a suspicious nature, reporting mandates are enshrined under the Financial Transactions Reporting Act, 2006. There are also requirements for monitoring transactions under the Prevention of Money Laundering Act. Although these statutes may not per se restrict access to all individuals, there is some level of restriction where transactions are suspicious and could fall within the ambit of any of these enactments.

133 **republicofsingaporeSriLankaSingapore2018?**

134 **SAFTA2004?**

135 Mutual Assistance in Criminal Matters Act 2002.

136 Mutual Assistance in Criminal Matters (Amendment) Act No 24 of 2018.

3 Deep dives

3.1 The Right to Information (RTI) Act and its implementation in Sri Lanka

The RTI legislation in Sri Lanka has been widely considered as a pathbreaking one, owing to the disclosure of information by public authorities (PAs) that has been made possible through the Act.[137] Prior to the passage of the Act, there was no legislation mandating disclosure of information.

3.1.1 RTI Disclosure of Information and Exemptions

In terms of Section 3 of the RTI Act, every citizen has the right to access information subject to the exemptions under Section 5 (1) of the RTI Act. Some of the exemptions are listed below-

There are several exemptions to access to information under Section 5 (1) of the RTI Act:

- Section 5(1)(a)- personal information
- Section 5(1)(b)- (i) territorial integrity / national security (ii) prejudicial to Sri Lanka's relation to international agreements
- Section 5(1)(c)- serious prejudice to the economy of Sri Lanka (exchange rates, regulation of banking/credit)
- Section 5(1)(d)- information including commercial confidence, trade secrets, protected under the Intellectual Property Act
- Section 5(1)(l)- harm the integrity of the examination being conducted by a Dept of Examination or higher educational institutions

It should be noted that even if an information request is within the ambit of these exemptions, where there is a public interest override under Section 5 (4) of the RTI Act, such public interest will prevail. There are several RTI Commission (RTIC) decisions that have evidenced increased transparency in the disclosure of information across sectors.[138]

Proactive Disclosure under the RTI Act

Sections 8, 9, and 10 of the RTI Act are the relevant provisions on proactive disclosure. Section 8 deals with a minister's duty to publish a report in electronic form and maintain it in physical form, relating to the functioning of the Ministry, budget, operations, and other relevant matters. Section 9 requires ministries to make all relevant details of new projects publicly accessible three months prior to the project's commencement. Section 10 requires all PAs to file annual reports with the RTIC. It should be noted that while Sections 8 and 9 only deal with Ministries, Regulation 20 issued under the RTI Act for proactive disclosure

[137] Natesan, "Towards Efficient Reporting Mechanisms for Enhancing Institutional Transparency."

[138] K.K.G Chandrika v. Office of the Director General of Health Services, Galle RTIC Appeal 2110/2020 ; W.R.M.F.H.A Walosundara v. District Secretariat, Gampaha RTIC Appeal 83/ 2017 ; Methsiri de Silva v District Health Service Office, Galle RTIC Appeal 1166 / 2019 ; M.J. Roche v Department of Immigration and Emigration RTIC Appeal RTIC Appeal 191 / 2018; G R M N B Rathnayake V. Central Environmental Authority RTIC Appeal(In-Person) /219/2018

requires all PAs, not just ministries, to submit, at the very minimum, information in relation to the institution, operation, budget, etc.[139]

A study conducted by a think-tank revealed that over 70% of PAs (only Ministries) had disclosed online less than 40% of the information they were required to by the RTI Act.[140] The Ministries of Agriculture and Public Administration, which ranked highest in the assessment, disclosed just over half of the required information. This indicates a low level of compliance among other PAs/Ministries. Importantly, the offices of the President and Prime Minister disclosed less than 20% of the required information and ranked among the least compliant, with the Ministry of Technology scoring the lowest overall.[141] The study also highlighted a significant language bias across most PAs. Only the Office of the President and the Ministry of Wildlife consistently published information online in all three languages. Overall, across all PAs, nearly half of all information online was disclosed in English, but only 37% was disclosed in Sinhala and just 29% in Tamil.[142] The 2024 study revealed that while only 6% of the PAs were found to be "moderately satisfactory" in 2017, the percentage had increased to 35% in 2024.[143] While compliance with proactive disclosure remains a significant concern, this improvement should not be overlooked. It should be noted that this study only examined proactive disclosure online, not whether information was maintained on physical premises. The RTI Act mandates that reports be made available in electronic form, and that physical copies be made available for public inspection.

An interview with the RTI Commissioner, Ms. Kishali Pinto-Jayawardena, revealed that capacity challenges were not the only reason for low levels of compliance. While she agreed that "a good e-governance system must be implemented," she added that "another reason is the in-built reluctance of state entities to be transparent. That requires attitudinal change."

A study has revealed that, as of 2019, 74% of PAs, 82% in 2020, and 78% in 2021, have failed to submit their annual reports in compliance with Section 10.[144] Another challenge in monitoring submission of PA (State sector) annual reports is that there is no directory containing the list of all State sector PAs in the country. When the RTI Commissioner, Ms. Kishali Pinto-Jayawardena, was questioned on these aspects, she reiterated the importance of having a directory, and for the nodal agency, namely the Media Ministry, to compile it. On the issue of poor compliance and monitoring of this statutory requirement of filing annual reports, she highlighted that while "…the Commission analyses the data as per the reports that come to us and calls upon PAs to submit in terms of their statutory duties. We cannot go further, for example, the Commission cannot prosecute on that basis. The Government must ensure that this duty is complied with."

These studies indicate that proactive disclosure levels are dismal in the country. The RTI regime in Sri Lanka primarily relies on reactive disclosures.

RTI and gender

The relevant forms to file RTI requests do not require disclosure of the gender of the requester. Even at the appeal stage before the RTI Commission, gender-disaggregated data

---

139 Regulations Promulgated Under the Right to Information Act, No. 12 of 2016.

140 Verite Research, *Proactive Disclosure Under the RTI Act in Sri Lanka: Ranking Public Authorities 2023.*

141 Verite Research.

142 Verite Research.

143 **ProactiveDisclosure2025?**

144 Verite Research, *Proactive Disclosure Under the RTI Act in Sri Lanka: Ranking Public Authorities 2023.*

are not required. It has thus proven to be difficult to assess the impact of RTI on gender/women's empowerment. A research study has documented several examples of women using RTI at the provincial level and how they have effected institutional changes in their own communities through the use of the RTI Act.[145] While these instances have not been recorded on a large scale, they have proven useful in establishing linkages between the use of RTI and gender-related benefits.

3.1.2 Friction points and how they are being dealt with

Research conducted by UNDP (2022) in Sri Lanka identified at least 105 existing legislations that were in conflict with the RTI Act.[146] In anticipation of this conflict, the drafters of the RTI Act included a specific clause in the Act: Section 4 states that in the event of an inconsistency or conflict between the RTI Act and any other written law, the RTI Act shall take precedence. The term 'written law' is not limited to legislation enacted by Parliament but also includes 'all orders, proclamations, rules, by-laws, regulations, warrants and process of every kind made or issued by anybody or person having authority under any statutory or other enactments.' This provision has been the subject of several appeals before the Commission. In the highly contested 2017 appeal of *Transparency International Sri Lanka v Presidential Secretariat*, the RTIC held that the RTI Act overrides the Declaration of Assets and Liabilities Law No. 1 of 1975.[147] The Order of the RTIC dealt with the declaration of assets by the then President and Prime Minister. The appeal is still pending in the Appellate Court.

In *Chamara Sampath v. Parliament of Sri Lanka,* the Appellant requested the list of names of Members of Parliament (MPs) who had submitted Declarations of Assets and Liabilities in 2018 and the list of names of MPs who had submitted such Declarations from 2010 until the date of the information request.[148] The Declaration of Assets and Liabilities Law requires MPs to disclose their assets and liabilities, but such information is confidential in nature and cannot be published. The RTI Act, on the other hand, provides for information to be disclosed unless it falls under one of the stated exemptions outlined in Section 5(1). In the appeal, the Commission *inter alia* rejected the argument made by the PA that information relating to declaration of assets and liabilities is 'personal information' of MPs which was protected from release in terms of Section 5(1)(a). The PA appealed to the Court of Appeal against the RTIC's order.

On an appeal, the Court of Appeal held in *Chamara Sampath v. Neil Iddawala* that the RTI Act would override the provisions of the Declaration of Assets and Liabilities Law No. 1 of 1975.[149]

Section 7(3) of the RTI Act requires that all public records be maintained for a period of not less than 10 years, while new records (those created after the RTI Act came into force) must be maintained for a period of not less than 12 years. This retention requirement poses an administrative challenge due to physical storage constraints and also potential conflict with the requirements under the National Archives Act. Currently, only some Directions on a roadmap for record keeping have been issued by the RTI Commission. When these points

145 Natesan, *Breaking Barriers: Women and Right to Information in Sri Lanka.*
146 **undpReviewLegislationConistency2022?**
147 *Transparency International Sri Lanka v Presidential Secretariat.*
148 *Chamara Sampath v. Parliament of Sri Lanka.*
149 *Chamara Sampath v. Neil Iddawala.*

were raised with the RTI Commissioner, it was emphasized that "The Commission is working with key Ministries to get these guidelines (on record management) out." The Strategic Implementation Plan (2017 to 2019) also included record management as a priority.

Thus far, the override provision, Section 4, has been used to give primacy to the RTI Act. However, there is cause for concern by virtue of the PDPA and other upcoming laws.

Conflict with PDPA

The RTI Act has an exemption on grounds of personal data. The section reads as follows:

> Section 5(1): Subject to the provisions of subsection (2) a request under this Act for access to information shall be refused, where (a) the ***information relates to personal information*** the ***disclosure of which has no relationship to any public activity or interest***, or ***which would cause unwarranted invasion of the privacy*** of the individual unless the larger public interest justifies the disclosure of such information or the person concerned has consented in writing to such disclosure; *(Emphasis added)*

The exemption clause encompasses protection of –

1. Disclosure of personal information that has no relationship to any public activity or interest or
2. Cause unwarranted invasion of privacy unless there is a larger public interest

This has been referred to as the *two-fold test* in the application of the exemption.[150]

Even without a PDPA, the PAs can rely on the above exemption to reject an information request. While there are no specific statistics on the number of requests rejected on grounds of Section 5(1)(a) of the RTI Act by PAs, a scan of the orders passed by the RTIC shows that a large number of requests, on which an appeal has been preferred relate to rejections by the PA under Section 5(1)(a) of the RTI Act.[151]

The RTI Act in Sri Lanka has a public interest override under Section 5(4), where even if personal information is involved, it can be disclosed, provided there is an overriding public interest. This public interest override is applicable to all exemptions under Section 5(1).

The burden of proof rests on the PA in establishing that the exemption is applicable. In cases of genuine invasion of privacy and no furtherance of larger public interest, the RTIC has ensured protection of privacy. (Section 5(1)(a) and Section 4)

The PDPA seeks to protect "personal data", which has been defined as follows under Section 56 of the said Act:

> "personal data" means, any information that can identify a data subject directly or indirectly, by reference to– (a) an identifier such as a name, an identification number, financial data, location data or an online identifier; or (b) one or more factors specific

---

150 **LegalCommentariesSelected2022?**

151 RTI Commission of Sri Lanka, *Selected Orders of the Right to Information Commission of Sri Lanka 2017-2018.*

to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural person.

The definition of "personal data" includes information about an individual that can identify such a person either directly or indirectly. There can be no dispute that this is a necessity. However, what is the situation when personal data is involved in an RTI request?

RTI requests routinely include vast amounts of personal data, particularly salary details. Would the application of PDPA mean that all personal data will be protected from disclosure?[152] How will these be disclosed in the future?

The Court of Appeal in a recent decision, *Litro Gas Lanka Limited vs. W.K.S. Karunarathne* considered the question of disclosure of salaries of officials in a PA under the Section 5(1)(a) exception.[153] Referring to "panopticon" / "anti-panopticon" it has been stated that the "Right to Information Act brings the state into the receiving end of asymmetrical surveillance and the citizens are placed in the central well of the "panopticon." The state now has to police itself for fear of punishment which it faces on adverse public opinion." It was held that disclosure of salaries under the RTI Act was thus necessary, and the decision of the RTIC was upheld.

Section 16 of the PDPA reads as follows:

16. Every data subject shall have the right to make a written request to the controller to have his personal data erased, under the following circumstances where(a) the processing of personal data is carried out in contravention of the obligations referred to in sections 5,6,7,8,9,10 and 11; (b) the data subject withdraws his consent upon which the processing is based, in accordance with item (a) of Schedule I or item (a) of Schedule II;

This right of data subjects, i.e., individuals, to request the erasure of information is referred to as the right to be forgotten. There have been case laws across the globe analyzing the right to be forgotten vis-à-vis freedom of information. While several judgments have given importance to the former, it has always been stated that the balance between the two would depend on the facts and circumstances of each case. The RTI Act does not require that reasons be given for an information request. However, under the PDPA, processing has to be for defined purposes

Additionally, Section 9 of the PDPA reads as follows:

9. Every controller shall ensure that personal data that is being processed shall be kept in a form which permits identification of data subjects only for such period as may be necessary or required for the purposes for which such personal data is processed:

Provided however, subject to the provisions of section 10 of this Act, a controller may store personal data for longer periods in so far as the personal data shall be processed

152 Natesan, *Right to Information Vs. Protection of Personal Data in Sri Lanka.*

153 *Litro Gas Lanka Limited vs. W.K.S. Karunarathne.*

further for archiving purposes in the public interest, scientific research, historical research or statistical purposes."

Under Section 7(3) of the RTI Act, all public records must be maintained for a period not less than 10 years, while new records (after the RTI Act came into force) must be maintained for a period not less than 12 years.

While the PDPA under Section 9 mandates that personal details should only be maintained for a period that is necessary or required for a specific purpose, the RTI Act mandates 10 / 12 years, as the case may be. The PDPA also allows for the personal data to be erased if the concerned individual withdraws their consent. In this scenario, can the PA be permitted to delete details of an inquiry report where the concerned person has withdrawn consent, or even fail to maintain the inquiry report, relying on the PDPA?

The Section 40 exemption clause of the PDPA is relevant in this context:

40. "Any exemption, restriction or derogation to the provisions of this Act shall not be allowed except where such an exemption, restriction or derogation is provided for in any law and respects the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society for —

(e) the protection of the rights and fundamental freedoms of persons, particularly the freedom of expression and *the right to information. (Emphasis Added)*

It is our view that even with an exemption clause, the situation of conflicts does not stand resolved.

3.1.3 RTI in Sri Lanka: Lessons for other jurisdictions

The RTI Act has been ranked 4th globally and 2nd in Asia on the Center for Law and Democracy's Global RTI index.[154]

That rating is based on 61 discrete indicators drawn from seven main categories– Right of Access, Scope, Requesting Procedure, Exceptions and Refusals, Sanctions & Protections, and Promotional Measures. The RTI Act came into being as a result of decades of campaigning and lobbying by civil society activists, media organizations, journalists, and lawyers. It is worth noting that, prior to the implementation of the RTI Act, the non-disclosure of information that adversely affected citizens was the norm in the country.

However, it is not that the legislation is without flaws. The record management requirements and proactive disclosure compliance levels are below satisfactory, and significant improvements are needed in these respects.

Development of the law

On the development of the RTI Bill, the RTI Commissioner has stated that "Speaking specifically regarding the RTI Bill in regard to which I served on the drafting committee,

[154] Centre for Law and Democracy and Access Info Europe, *Global Right to Information Rating*.

there was an extensive period of consultations by a committee comprising experts, all suggestions and recommendations by external parties were taken into account."

It has been noted that even with consultations, some conflicts arise. The RTI Commissioner was also questioned on challenges in record management and retention. She categorically responded that "the main challenge is the statutory time limits prescribed for retention. The Commission cannot change this as it is in the statute. But PAs have a major problem in adhering to that rule due to a lack of storage space/lack of resources. After extensive discussions, the Commission is attempting to limit the meaning of the term 'record' used in Section 7 and will attempt to draw up guidelines to that effect, provided that consensus is reached."

When the RTI Commissioner was questioned on whether they were consulted during the drafting of the various laws, the response was that "No, the Commission has not been consulted at the drafting stage of the laws." Furthermore, adding that "Future laws that limit the reach of the RTI Act must not be enacted by the Government and bodies entrusted with framing policies and rules concerning new anti-corruption, anti-terrorism and privacy legislation must take this concern into mind."

Capacity challenges

When the question of capacity challenges was raised to the RTI Commissioner, her response was "Primarily the RTI Commission must have an independent line item in the National Budget which the Commission had during 2017, but it was changed thereafter to bring the funding under the Media Ministry. The issue is not so much the lack of money but the non-independent manner in which the funds are processed to the Commission. This must be rectified."

It has been observed that even at the PA level, there are several capacity challenges. When the RTI Commissioner was questioned on this she responded that "the batch of IOs [Information Officers] extensively trained when the RTI Act came into operation (2017) have now been transferred out and new batches have been appointed who have no/little knowledge of the RTI Act/Regulations/ procedures" when further questioned as to how this could be improved she responded that "the performance of the nodal agency which is the Ministry of Media, must be vastly improved so that there is a) training of IOs b) capacity checks to see if these trainings are done properly without just being 'tick-in the box' exercises."

While the RTI regime in Sri Lanka has been a landmark in its legislative history for transparency, the challenges, especially those surrounding capacity building, proactive disclosures, retention of records, and conflict with upcoming laws, remain writ large.

3.2 PDPA in Sri Lanka – What lies ahead

The PDPA is not yet in force (substantial provisions come into force in March 2025), and as such, it is necessary to analyze the various provisions under the PDPA.

Exceptions to processing data without consent

In general, data can only be processed with the consent of the data subject or subject to the fulfillment of other conditions for lawful processing, such as legitimate interest or being

necessary for the performance of a contract. However, if data is required on grounds of public interest (such as health, control of communicable diseases, or compliance with law), it can be processed without the consent of the data subject. Specifically, under Section 40 of the PDPA, exemptions, restrictions, or derogations to the PDPA would be permitted, *inter alia*, for the following reasons:

- the protection of national security, defense, public safety, public health, economic and financial systems stability of the Republic of Sri Lanka;
- the impartiality and independence of the judiciary;
- the prevention, investigation and prosecution of criminal offences;
- the execution of criminal penalties.
- Freedom of expression and right to information

It is essential to emphasize that there is no exemption for journalistic processing of personal data.[155] Although this has been subject to criticism and early drafts highlighted this issue, it remains the case.[156]

3.2.1 Data Protection Authority

The Data Protection Authority (DPA) plays a crucial role in implementing the PDPA. It is pertinent to highlight that an early draft of the Bill specifically called for the appointment of 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."[157] Commendably, this "government-controlled" reference was removed. In terms of Section 29 of the PDPA, the "administration, management and control of the affairs of the Authority shall be vested in a Board of Directors". The qualifications of the Board and appointment of the Chairperson have been included in the PDPA. In an interview with Mr. Jayantha Fernando, Member of the Board of Directors appointed under the PDPA, who previously was involved in the drafting of the legislation, emphasized how the legislation included qualifications of the Members of the Board of Directors and that it was an important step towards transparency.

3.2.2 Cross-border transfer of data

The PDPA (as it currently stands) has approached cross-border transfers differently for "public authorities" and those from the private sector. The PDPA states that a "public authority" means, "a Ministry, any Department or Provincial Council, local authority, statutory body or *any institution established by any written law,* or a Ministry, any Department or other authority or institution established or created by a Provincial Council" (hereinafter "State entities"). It should be mentioned that in an earlier draft of the Personal Data Protection Bill, the "public authorities" definition included a reference to "a company registered under the Companies Act, No. 7 of 2007 in which the government or a public corporation or a local authority directly holds fifty per centum or more of the shares

155 Natesan, "Is the Proposed Data Protection legislation a cause for concern for journalistic expression?"
156 *Daily Mirror*, "Personal Data Protection Bill."
157 The Personal Data Protection Bill, 2019.

of that company."[158] But this has been removed in the subsequent draft. It is pointed out that the present definition makes a mention of "any institution established by any written law," this may cause some confusion as to the nature of entities included for example would privately owned banks or financial institutions established under the Banking Act and Finance Business Act be included? It can be argued that the provision has to be read as a whole and applying the statutory interpretation rules of *noscitur a sociis* (meaning should be inferred by reference to other words in the context) and *ejusdem generis* (of the same kind), this reference could only mean State entities and not private ones. Notwithstanding this, there is still room for ambiguity. This is relevant since these public authorities / State entities are required to store personal data locally. During the interview with Mr. Jayantha Fernando, this position was affirmed and it was highlighted that it is clear that the intention was to remove public corporations and other such entities.

The proposed amendment to the PDPA has clarified this position. The definition of "public authority" only includes a Ministry, any Department or Provincial Council, local authority, or a Ministry or Department of Provincial Council, but does not include a public corporation or a company incorporated under the Companies Act.

The proposed amendments have also excluded the requirement of "adequacy decision" for both public authorities and private entities.

As per the proposed amendment, there can be a cross-border transfer of personal data

- where such controller or processor ensures compliance with the obligations imposed under Part I, Part II, and Sections 20, 21, 22, 23, 24, and 25 of Part III of the PDPA; or
- where appropriate safeguards mentioned in point two above, a controller or processor other than a public authority may process personal data outside Sri Lanka in certain special instances listed in Section 26(5) i.e. explicit consent; transfer is necessary for the performance of a contract; necessary for establishment of legal claims; transfer in public interest; emergency situations such as health emergency; other conditions as maybe prescribed by regulations.

Web Scraping and Publicly Available Data

The PDPA does not specifically mention that "publicly available data" or that obtained from public sources are exempt from its application. However, under Schedule V (Collection of Personal Data), it has been stated that where personal data has been collected by means other than direct interaction with the data subject, details of such collection of data, including the source of the data, must be provided to the data subject. It can be inferred that web scraping can be done, provided the data subject is informed of this. Providing such notice is, of course, impossible when one is scraping billions of web pages. There is a potential exemption that could be relied upon by controllers in such cases, which reads as follows: "the provision of such information proves impossible or would involve a disproportionate effort."

While the lawful bases for processing of data in Sri Lanka include "legitimate interests" and the explanation for the same includes instances where "a data subject reasonably expects at the time and in the context of the collection of the personal data that processing for that purpose may take place", as under Schedule V (Collection of Personal Data), the legitimate

[158] The Personal Data Protection Bill, 2019.

interest pursued by the Controller should be disclosed to the data subject. There is an exception to this requirement of notice, i.e. where providing such information would be impossible or would involve disproportionate effort. Although this exception specifically refers to "processing for archival purposes," it could potentially be extended to web scraping.

3.2.3 Friction with other laws

During the interview with the DPA Board member, the question was raised on potential conflicts with other laws, such as the National Archives Act. The response was very encouraging, stating that "extensive consultations will be held with RTI Commissioners, Advisory Committees will also be appointed to study the potential conflicts with laws like the RTI and National Archives; there will be engagement with these regulators, and steps will be taken to work together".

Since we are still in the early stages of the Board coming into operation, these efforts have not yet been reported. The proposed amendments, including the postponement of the PDPA, have also put a pause on these initiatives.

3.2.4 Lessons for other jurisdictions

The PDPA text has been lauded by some experts, indicating that it falls in line with international standards.[159] The PDPA follows the GDPR blueprint; it has been repeatedly stated that following the GDPR model would increase Sri Lanka's trade relations and also ensure "adequacy" of its laws. In a welcome move, the proposed amendments to the PDPA exclude the requirement of an "adequacy decision."[160]

There is some concern that the other appointments under the DPA could be subject to political interference and be tainted by bias.[161] The process of passing the law and conducting public consultations is worthy of replication, and it can be deemed a good practice. Notwithstanding this, the outcomes of public consultations have not been published, which could be seen as a step closer to enhancing transparency. It is also commendable that international partners are being consulted in setting up the DPA. The interview with the DPA Board Member confirmed this.

3.3 Development of laws

It is worth noting that consultations were held with stakeholders during the drafting of the legislation. It is also understood that meetings/discussions were conducted with relevant institutions.[162] The Drafting Committee of the Bill comprised persons from both the public and private sectors, including representatives from two telecommunication operators.[163] There was criticism that the proposed amendments were not subject to public consultation before being published. While the drafting process was transparent, with members of the

159 Walpola, *"Implementation of Personal Data Protection Act Likely to Be Hampered by Political Interference"*.

160 *Daily FT*, "How Best to Keep Data Safe (and Drive the Digital Economy)?"

161 Walpola, *"Implementation of Personal Data Protection Act Likely to Be Hampered by Political Interference"*.

162 *The Morning*, "Data Protection Bill Further Delayed."

163 *The Morning*, "Data Protection Bill Further Delayed."

same being made public and consultations also taking place, there are still some concerns and potential conflicts with other laws as aforementioned.

3.3.1 Capacity challenges

In light of Sri Lanka's economic hardships in 2022 and subsequent resource limitations, the capacity challenges in implementing the PDPA hardly require elaboration. It would be a challenge for both the public and private sectors. When this question was put forth to the DPA Board member, it was stated that "while there are many capacity challenges, the government could work with institutions like SLIDA [Sri Lanka Institute of Development Administration] to embark on training and capacity building. Furthermore, countries like the Philippines, Indonesia, and Thailand have formulated plans/budgets for setting up such systems, which can be replicated. Particularly, it is necessary for the DPA to be a revenue-generating body with proper structures." It should be noted that in terms of the PDPA, penalties paid are credited to the Consolidated Fund and there is no specific fund for the DPA. The Board Member also emphasized policy-level strategic guidance for developing budgets to enhance capacity.

3.4 Summary of findings

1. What are the implications of the emergent nature of the governance architecture? Because there is no overall design that envisions how the parts fit together, it is likely that there will be friction points and even contradictions. How are these being worked out?
    - Laws restricting access to information have been widely used on grounds of national security. (For example, SLTA and the Computer Crimes Act.)
    - Conflicts and inconsistencies between laws, in relation to data governance, are typically not remedied through amendments, but subsequent laws tend to have a provision on non-obstante/overriding effect. For example, the Online Safety Act has a non-obstante clause. However, the proposed amendments to the PDPA stand as an exception.
    - It is understood that the PDPA Board would establish advisory committees with other stakeholders to ensure potential conflicts with other laws are ironed out. Still, such practices are not uniform across sectors.
    - The forthcoming national archives law is making an effort to expressly remedy conflicts with other laws, such as the PDPA.
2. The emerging governance architecture involves tradeoffs among objectives such as greater accountability of powerholders, economic growth, including the creation of employment and wealth, resilience of systems, etc. How has Sri Lanka: (a) explicitly recognized the tradeoffs or not; and (b) handled them?
    - It can be observed that there are some sectoral differences, for example, the financial sector regulations are not fully consistent with the general framework on cross-border data under the PDPA.

- The policies under the health sector are also varying and multifold, but they have not been analyzed in this study due to the absence of common structures.
- The "Connected Government" initiative includes use cases of potential conflicts and also other concerns, but efforts have not been taken to remedy the concerns, and it remains a theoretical piece.
- The analysis above shows that there has been limited explicit recognition of tradeoffs. The draft policies have a wide-ranging impact, but the realities of implementation have not been considered.
- Sector-specific considerations should not be ignored. For example, agreements relating to financial matters have been excluded from the application of the Electronic Transactions Act. However, the CBSL has also not independently addressed this, and this statutory lacuna remains unresolved.

3. Are there legislative or policy innovations with potential for replication? What are the modalities of sharing experiences? Is Sri Lanka learning from other developing countries, or is it learning from the developed countries?
   - The RTI Act in Sri Lanka and its implementation have been laudable. There have been several orders of the RTI Commission to substantiate its effectiveness in the country. Notwithstanding its successes, some areas require significant improvement, particularly record management and proactive disclosure.
   - There have been no uniform practices in Sri Lanka on replication from other countries. Some policies have mentioned that they are based on laws from different countries; for example, the Minimum Information Security Standards have taken guidance from New Zealand, and the PDPA has followed the EU GDPR model.
4. How were the laws and bills developed? What expertise was brought to bear? How open were the procedures? How receptive were drafters to suggestions and criticisms?
   - Sri Lanka has had some documented history of public consultation in passing laws, but the recent legislation, the Online Safety Act, No. 09 of 2024, has shown that such efforts are not uniform. The Act was passed with limited to no consultation and passed without following the necessary procedures.
   - Sri Lanka has numerous policies, strategies, and discussion papers on data governance, but many are still in draft form or are formulated in silos. When the DPA Board Member, formerly General Counsel of ICTA, was questioned on this, he stated that "the e-Sri Lanka initiative was initially formulated to bring an integrated structure in place; however, the lack of an enforcement mechanism was a key drawback".
   - The existing structure is fragmented and confusing since there is no central coordination and implementation.
   - Data Governance is gaining priority with specific mention under the National AI strategy. The Ministry of Digital Economy is also focusing on data governance. It is understood that the data sharing policy and other related drafts will be considered, and amendments will be made accordingly.
   - The necessity to have interoperability is widely recognized across policies, including in the draft Cloud Strategy and Cloud Policy, but there has been limited

implementation. The National Enterprise Architecture outlines the potential for interoperability; however, large-scale cooperation is lacking.

5. How were capacity challenges addressed: by simplifying the laws or by tolerating incomplete implementation?
    - The focus areas of RTI and PDPA indicate that capacity challenges continue to be a concern in the implementation or proposed implementation of the laws.
    - The "Connected Government" initiative has a recommendation document on how capacity can be overcome, but it appears that much progress has not been made on that front.
    - The regulatory bodies have tried to simplify the framework in some respects, such as archiving requirements by the RTI Commission, but this is not uniform across sectors.

4 Concluding thoughts

The report emphasizes the significance of data governance in shaping Sri Lanka's digital future. While progress has been made through some laws and policies, there is still much to be done. Institutional capacity constraints, conflicting laws, and gaps in implementation are the hurdles to a cohesive governance framework. To address this, we need to work together to build institutional resilience, inter-agency collaboration, and training for public officials. Additionally, take steps to submit the action plan to revive membership at the OGP.

A 2017 report of the UNDP on Sri Lanka stated, "More challenging will be to change the underlying institutional culture regarding data use to more systematically utilize data *for planning and addressing multi-dimensional challenges.* This will require not only strengthened capacities in relevant institutions, but *also developing new, innovative methods for data collection and demonstrating the value of evidence-based policymaking*"[164] (Emphasis added).

This remains relevant even today; the National Fuel Pass demonstrates how effectively utilizing data can bring about positive societal change to help address urgent challenges, such as resource optimization. It underscores the potential of data-driven solutions to transform governance and public service delivery. Sri Lanka must prioritize not only the effective use of existing data and clear policies to aid such use but also the establishment of reporting structures that reduce bureaucratic delays.

4.1 Recommendations

4.1.1 Legal and Policy Coherence

Harmonize Conflicting Laws and policies

- Conduct a comprehensive legal audit to identify overlaps/conflicts between sectoral laws (e.g., PDPA, RTI Act, Telecommunications Act, Computer Crimes Act, etc.) and policies
- Requiring cross-referencing clauses in all new policies impacting data governance.

Establish a Unified Framework for Data Governance (as proposed in the National AI Strategy)

- Establish a framework to guide inter-agency coordination, define roles, and outline enforcement mechanisms for data governance.
- Finalize and operationalize pending draft policies (e.g., Data Sharing Policy, Interoperability Framework).
- Digital Public Infrastructure needs more focus and policy articulation.

4.1.2 Institutional and Structural Reforms

Strengthen the Institutional Coordination Mechanism

- Require sector regulators (e.g., CBSL, DPA, RTIC, National Archives, etc.) to work collaboratively and ensure alignment with national frameworks.

[164] **undpCountryProgrammeDocument2017?**

Empower and Operationalize Advisory Committees

- Ensure sector-specific advisory committees under the PDPA Board are established and functional.
- Institutionalize their recommendations through rules or guidelines with public consultation for transparency.

4.1.3 Implementation and Capacity Building

Develop a National Capacity Building Roadmap

- Tailor training modules for public officials, segmented by agency roles (e.g., data controllers, processors, archival officers, RTI officers).
- Implementation of initiatives like GovPay requires rigorous and continuous training.

Address Fragmentation Through Shared Platforms

- Accelerate the implementation of the National Enterprise Architecture and the implementation of the Lanka Interoperability Framework.

4.1.4 Public Engagement and Transparency

Institutionalize Meaningful Public Consultations

- Making public consultations a prerequisite for all laws and policies, including those related to digital/data governance, with a standard consultation period and reporting mechanism.
- Set up a mechanism such as a "consultation tracker" to reflect how stakeholder feedback was incorporated.

Increase Public Awareness and Civic Participation

- Launch awareness campaigns about citizens' rights under laws like the RTI Act and PDPA.
- Engage and educate regarding citizen-centered initiatives like the unique Digital ID.

4.1.5 Monitoring and Evaluation

Periodic Review of Laws and Policies

- Build a periodic review mechanism into all future data-related laws to ensure relevance and responsiveness.

A mechanism to conduct reviews

- A framework on how the laws will be reviewed and by which agency should be clearly established.

Annexure

Annex 1: Policy Objectives: National Digital Government and Governance Policy

Policy Objective	Details
Easy Access	**a. Government Services Aggregator** • Present services through www.gov.lk, in three languages (mandatory) **b. Digital Channels and Social Media** • Use digital channels and social media for dynamic information sharing • Verified social media profiles and governing policies **c. Internal Mechanisms** • Compile, collect, translate, and provide updated information **d. Proactive Information Disclosure** • Adhere to Right to Information principles and Data Protection Act No. 09 of 2022 • Disclose relevant information in official languages **e. Digital Availability of Documents** • Make all forms, guidelines, circulars, and artifacts available digitally for download
Common ICT Infrastructure / Interoperability	**a. National Data Exchange (NDX)** • Implement APIs for third-party and private entity data consumption • Aim for cost savings, efficacy, and efficiency **b. National Spatial Data Infrastructure (NSDI)** • Facilitate interoperability and collaboration among government organizations

Policy Objective	Details
	• Standardize spatial data, avoid duplication, improve quality, and transparency **c. Identity Interoperability Platform** • Digitally validate identities for services like driver's licenses • Access necessary data (birth, health, etc.) for identity confirmation **d. Shared Solutions** • Utilize shared solutions for operations like email, payroll, HR management, and payments • Design, develop, and use service providers for these solutions **e. Lanka Government Network (LGN) and Other Infrastructures** • LGN for data sharing among government organizations • Middleware infrastructure, Lanka Government Cloud (LGC), Mobile Portal, GovSMS, Lanka Government Payment Service, and Government Information Centre (GIC) **f. Lanka Interoperability Framework (LIFe)** • Open standards for operability • Provide services through a single window in domains like Personal, Land, Vehicle, and Project Coordination

Annex 2: Draft Policies under Digital Government

Policy	Details
National Data Sharing Policy (Draft, 2013)[165]	• **Objective:** for "open government" and to "create an integrated platform to enable seamless sharing of information to the right people at the right time in a secure, reliable manner to promote mutual

[165] **ictasrilankaNationalDataSharing2013?**

Policy	Details
	benefits to individuals, civil society and the country" • **Applicability:** All data created, generated, collected, or archived by the government. • **Key Components:** • **Data Classification Framework:** Based on the impact of sharing information with different stakeholders. • **Service Classification Framework:** Shares Information Assets as Data Services or Verification Services, classified as Open, Authorized, or Restricted. • **Data Sharing Policy:** Specific policies for departments to implement effective information sharing. • **Data Retention:** Data should be retained for a "minimum period", then destroyed or downgraded.
Government Cloud Policy[166]	**Underlying requirement:** Government entities are recommended to use the Lanka Government Cloud; third-party cloud services can be used with ICTA approval, and where their requirements cannot be satisfied by the government Cloud. **Requirements to be fulfilled by the third-party Cloud Service Provider (CSP)** • **Private Cloud:** Dedicated for government use. • **Certifications Required for CSPs:** • ISO/IEC 27017 • NIST SP 800-53 • Level 2 of CSA STAR • **Data Centre Certification:** Tier 3.

[166] Information and Communication Technology Agency of Sri Lanka, "Government Cloud Policy – Draft v 1.7."

Policy	Details
	• **Breach Notification:** CSP must notify the government within 24 hours of a breach.
Digital Document Management Policy[167]	• **Goal:** Shift from paper to digital document management. To increase Efficiency, productivity, accountability, interoperability, and meeting citizen expectations. • **Approach:** Create, maintain, disseminate, and destroy electronic records consistently. • **Document Retention:** In line with RTI Act; system administrator decides on purging, archiving, or copying files. • **Note:** No mention of national archives laws.
Information Classification Framework[168]	• **Purpose:** Document and illustrate the Information Classification Framework for government organizations. Towards open data and information sharing. • What, why, and how of information classification; framework and implementation.
Information Classification Policy[169]	• **Objective:** Recognize and classify information assets based on significance and sensitivity. • **Impact Levels:** From low to very high, depending on consequences in the event of a breach.

Annex 3: Cyber Security Strategy Thrust Areas

Objective	Details
1. Establishment of Governance Framework	• Implement a governance framework for the National Information and Cyber Security Strategy.

[167] **DigitalDocumentManagement?**
[168] Information and Communication Technology of Sri Lanka (ICTA), *Sri Lanka Government Information Classification Framework (SLGICF).*
[169] **InformationClassificationPolicy?**

Objective	Details
2. Enactment and Establishment of Legislation, Policies and Standards	• Formulate laws, policies, and standards to create a regulatory environment for cyber security.
3. Development of Competent Workforce	• Develop a skilled workforce capable of detecting, defending, and responding to cyber-attacks.
4. Resilient Digital Government and Infrastructure	• Ensure digital government systems have appropriate cyber security and resilience by working with public sector authorities.
5. Raising Awareness and Empowerment of Citizens	• Educate and empower citizens to protect their identity, privacy, and economic assets in cyberspace.
6. Development of Public-Private, Local International Partnerships	• Foster partnerships between public and private sectors, locally and internationally, to enhance cyber security.

References

"AIC Warns Sri Lanka's Online Safety Bill Threatens Freedom of Expression." *Digital Watch Observatory*, October 4, 2023. https://dig.watch/updates/aic-warns-sri-lankas-online-safety-bill-threatens-freedom-of-expression.

Anti Corruption Act 2023. Accessed December 8, 2024. https://parliament.lk/uploads/acts/gbills/english/6296.pdf.

Banking Act Directions, Pub. L. 16 of 2021 (2021). https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/Banking_Act_Directions_No_16_of_2021.pdf.

C. Kodeeswaran v. Attorney-General, Privy Council Appeal No. 38 of 1968, S. C. 408 | 64, D.C. Colombo, 1026 | Z (1969). https://lankalaw.net/wp-content/uploads/2024/12/073-NLR-NLR-V-72-C.-KODEESWARAN-Appellant-and-THE-ATTORNEY-GENERAL-Respondent.pdf.

Centre for Law and Democracy, and Access Info Europe. *Global Right to Information Rating*. 2023. https://web.archive.org/web/20240812115711/https://www.rti-rating.org/rating/. https://www.rti-rating.org/rating/.

Chamara Sampath v. Neil Iddawala (2018).

Chamara Sampath v. Parliament of Sri Lanka (2018). https://www.rticommission.lk/web/images/pdf/08022021/719-2018.pdf.

Committee on Formulating a Strategy for Artificial Intelligence (CFSAI). *Artificial Intelligence in Sri Lanka*. 2024. https://mot.gov.lk/assets/files/AI%20White%20Paper%20March%202024-c09aa49f7990358ad1442103b804511d.pdf.

Constitution of the Democratic Socialist Republic of Sri Lanka (2023). https://www.parliament.lk/files/pdf/constitution.pdf.

Cooray, L. J. M. *An introduction to the legal system of Sri Lanka*. Stamford Lake Publication, 2011.

Credit Information Bureau of Sri Lanka Act No: 18 of 1990 (1990).

"CRIB Score Reports - Individual | Credit Information Bureau of Sri Lanka." Accessed June 25, 2024. https://www.crib.lk/en/our-services/credit-information-services-for-the-general-public/crib-score-reports-individual.

Daily FT. "How Best to Keep Data Safe (and Drive the Digital Economy)?" March 27, 2025. https://www.ft.lk/columns/How-best-to-keep-data-safe-and-drive-the-digital-economy/4-774812.

Daily FT. "The rule of law." September 3, 2021. https://www.ft.lk/columns/The-rule-of-law/4-722553.

Daily Mirror. "Personal Data Protection Bill: Another draconian law to suppress media freedom?" 2022. https://www.dailymirror.lk/print/news-features/Personal-Data-Protection-Bill:-Another-draconian-law-to-suppress-media-freedom-/131-233442.

DataDissaPolicy2007. Accessed January 9, 2024. http://www.statistics.gov.lk/Datadessiminat ion/DataDissaPolicy_2007Oct26.

Democratic Socialist Republic of Sri Lanka, and Sri Lanka CERT. *Sri Lanka National Information and Cyber Security Strategy 2019-2023.* 2018.

"Department of Census and Statistics." Accessed January 30, 2024. http://www.statistics.gov.lk/.

"Department of Census and Statistics." Accessed January 30, 2024. http://www.statistics.gov.lk/Datadessimination#gsc.tab=0.

"Department of Census and Statistics." Accessed January 30, 2024. http://www.statistics.gov.lk/about_us/censusordanance#gsc.tab=0.

Department of Commerce, USA. "Sri Lanka Country Commercial Guide." International Trade Administration. Accessed July 5, 2023. https://www.trade.gov/country-commercial-guides/sri-lanka-trade-agreements.

Department Survey Regulations (2020). https://www.survey.gov.lk/sdweb/pdf/surveydocuments/DSR_6th_EDITION/DSR_English_6thEdition.pdf.

Dialog Axiata PLC. "Dialog Axiata, MIT and ICTA Recognised by the Ministry of Power…." Accessed March 3, 2024. https://www.dialog.lk/news/dialog-axiata-mit-and-icta-recognised-by-the-ministry-of-power-and-energy-for-implementation-of-the-national-fuel-pass-platform.

"Digital ID Launch by 2026: A Big Step Toward a Modern Sri Lanka." Ministry of Digital Economy, n.d. Accessed September 4, 2025. https://mot.gov.lk/assets/files/DOCE-7285826ba315a554a816d31269c24b9b.pdf.

Draft National Policy on Archives and Records Management v 1.2 (2023). https://www.archives.gov.lk/web/images/pdf/2023/draft_national%20policy%20on%20archives%20and%20records%20management_v1.2_english.pdf.

"Draft Revised Cloud Policy and Procurement Guidelines for Interim Use." 2025.

E-Government Policy- Draft (2014). https://www.gov.lk/elaws/wordpress/wp-content/uploads/2015/03/eGov-Policy-structured-v4-0.pdf.

Electronic Transaction (e-Registration of Persons) Regulations No. 1 of 2019 (2019). https://www.icta.lk/icta-assets/uploads/2020/06/Electronic-Transactions-Act-Regulations-2.pdf.

Electronic Transactions Act Amendment 2017 (2017). https://www.srilankalaw.lk/YearWisePdf/2017/25-2017_E.pdf.

Fernando, Shenal. "New Digital Transformation Agency to Absorb ICTA." *The Morning*, May 26, 2024. https://themorning.lk//articles/fxQ5CxAKxBZvsMuZZRCT.

"Finance Business Act Direction No 1 of 2022." 2022. https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/snbfi_finance_business_act_directions_no_01_of_2022_e.pdf.

Framework for National Archives and Records Management Legislation (2024).

Gazette on Operation of Personal Data Protection (2024).

Good Governance. "12 Principles of Good Governance - Good Governance - Www.coe.int." Accessed November 11, 2023. https://www.coe.int/en/web/good-governance/12-principles.

Google Docs. "Stakeholder Consultation on Sri Lanka's National Digital Economy Strategy." Accessed November 9, 2023. https://docs.google.com/forms/d/e/1FAIpQLSca7ZzVJKwF07lUNCF8pL4M997F5t77e_43iH_Oj03sAJWb3Q/viewform?usp=send_form&usp=embed_facebook.

GovPay. "Pay Traffic Fines Online with GovPay." GovPay. Accessed November 11, 2025. https://govpay.lk.

GovPay. "Secure & Convenient Payments." GovPay. Accessed November 11, 2025. https://govpay.lk.

Gunatilleke, Gehan. *A Rights-Based Approach to Limitation Clauses in the Sri Lankan Constitution*. no. 9 (2016).

Hassim, Imthiyaaz. "My First Experience with GovPay." 2025. https://www.linkedin.com/feed/update/urn:li:activity:7368212272382476290/.

"Home | NCOSC." Accessed November 11, 2025. https://ncsoc.gov.lk/.

ICTA. "Public Consultation: Call for Views on Cloud Policy and Strategy for Sri Lanka." Accessed November 11, 2025. https://www.icta.lk/.

Information and Communication Technology Act No. 27 (2003). https://www.icta.lk/icta-assets/uploads/2016/03/Information_and_Communication_Technology_Act_No.27.pdf.

Information and Communication Technology Agency of Sri Lanka. "Government Cloud Policy – Draft v 1.7." 2022.

"Information and Communication Technology Agency of Sri Lanka." Accessed November 11, 2023. https://www.icta.lk/.

"Information and Communication Technology Agency of Sri Lanka." Accessed November 11, 2023. https://www.icta.lk/.

"Information and Communication Technology Agency of Sri Lanka." Accessed March 3, 2024. https://www.icta.lk/.

"Information and Communication Technology Agency of Sri Lanka." Accessed December 8, 2024. https://www.icta.lk/.

Information and Communication Technology of Sri Lanka (ICTA). *Sri Lanka Government Enterprise Architecture: The Whole of Government Approach*. Version 1.0. 2023.

Information and Communication Technology of Sri Lanka (ICTA). "Sri Lanka Government FOSS Adoption Draft." 2022. https://www.icta.lk/icta-assets/uploads/2022/05/Sri-Lanka-Government-FOSS-Adoption.pdf.

Information and Communication Technology of Sri Lanka (ICTA). *Sri Lanka Government Information Classification Framework (SLGICF)*. 2015. https://www.gov.lk/elaws/wordpress/wp-content/uploads/2015/08/Information_Classification_FW_Report-v3-1.pdf.

Intellectual Property Act, Pub. L. 36 (2003).

"Invitation to Provide Input on National Digital Economy Strategy | Ministry of Technology." September 27, 2023. https://mot.gov.lk/blog/national-digital-economy-strategy.

Karunasena, Sanjaya, Samisa Abeysinghe, Dr. Hans Wijayasuriya, and Harsha Purasinghe. *Towards a Sovereign Cloud Strategy for Sri Lanka: A Government-Regulated, Private-Sector-Driven Approach to Enable Local Innovation and Trusted International Collaboration.* Version 0.4. 2025.

"Lanka Datta." Accessed February 19, 2024. https://nada.statistics.gov.lk/index.php/home.

"LankaSign Certification Service Provider (CSP) | Knowledge Center - Lanka Clear." Accessed November 11, 2023. https://www.lankapay.net/knowledge-center/lankasign/.

LBO. "Online Safety Act: Transparency International Sri Lanka Demands Corrective Action." Elections. *Lanka Business Online*, February 6, 2024. https://www.lankabusinessonline.com/online-safety-act-transparency-international-sri-lanka-demands-corrective-action/.

Litro Gas Lanka Limited Vs. W.K.S. Karunarathne (2024).

"Minimum Information Security Standards." 2021. https://www.onlinesafety.lk/wp-content/uploads/2021/07/Minimum_Information_Security_Standards_Version1_14-07-2021.pdf.

Mohamed Razik Mohamed Ramzy v. B.M.A.S.K. Senaratne (2023). https://www.supremecourt.lk/images/documents/sc_fr_135_2020.pdf.

Mutual Assistance in Criminal Matters Act 2002 (2002). https://www.imolin.org/doc/amlid/Sri_Lanka_MLA.pdf.

Mutual Assistance in Criminal Matters (Amendment) Act No 24 of 2018 (2018). https://www.moj.gov.lk/images/pdf/other/amend24-2018_E.pdf.

Natesan, Ashwini. *Breaking Barriers: Women and Right to Information in Sri Lanka.* Sri Lanka Press Institute, 2025.

Natesan, Ashwini. "Is the Proposed Data Protection legislation a cause for concern for journalistic expression?" *Daily FT*, June 2, 2021. https://www.ft.lk/columns/Is-the-Proposed-Data-Protection-legislation-a-cause-for-concern-for-journalistic-expression/4-718683.

Natesan, Ashwini. *Right to Information Vs. Protection of Personal Data in Sri Lanka.* 2023.

Natesan, Ashwini. "Towards Efficient Reporting Mechanisms for Enhancing Institutional Transparency." In *Sri Lanka's Right to Information Regime and the United Nations Sustainable Development Goals: Thoughts For Reflection.* 2022.

"National AI Strategy for Sri Lanka." 2024.

National Archives Law, No. 48 of 1973 (1973). https://www.lawnet.gov.lk/national-archives-law-2/.

National Digital Government/Governance Policy for Sri Lanka. Accessed November 11, 2023. https://www.icta.lk/icta-assets/uploads/2023/10/national-digital-government-and-governance-policy-for-sri-lanka_v-4.5_english.pdf.

Newswire. "Online Safety Act : Businessman Punished for Posting Fake News Against Former Minister." News. November 28, 2024. https://www.newswire.lk/2024/11/28/online-safety-act-businessman-punished-for-posting-fake-news-against-former-minister/.

OECD. *Going Digital Guide to Data Governance Policy Making.* OECD, 2022. https://web.archive.org/web/20231116075558/https://www.oecd-ilibrary.org/science-and-technology/

going-digital-guide-to-data-governance-policy-making_40d53904-en. https://doi.org/10.1787/40d53904-en.

"Online Registered Vehicle Information Service - Department of Motor Traffic - Sri Lanka." Accessed December 8, 2024. https://eservices.motortraffic.gov.lk/VehicleInfo/home.action.

Online Safety Act No 9 of 2024 (2024). https://www.parliament.lk/uploads/acts/gbills/english/6311.pdf.

"Open Data Portal - Sri Lanka." Accessed December 8, 2024. https://data.gov.lk/.

"Paris Convention for the Protection of Industrial Property." 1973. https://www.wipo.int/treaties/en/ip/paris/index.html.

"Payment and Settlement Systems." 2020. https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/Payment_and_settlement_systems_circular_no_13_of_2020_e.pdf.

"Payment and Settlement Systems Circular No 6." 2018. https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/Payment_and_settlement_systems_circular_no_06_of_2018_e_0.pdf.

Perera, Binendri. *Semi-Presidentialisation and Executive Accountability: A Cautionary Tale from Sri Lanka to the UK*. The Constitution Society, 2024. https://consoc.org.uk/wp-content/uploads/2024/06/Semi-Presidentialisation-and-Executive-Accountability.pdf.

Personal Data Protection Authority progresses with Board appointment | Daily FT. October 2023. https://www.ft.lk/front-page/Personal-Data-Protection-Authority-progresses-with-Board-appointment/44-753871.

Presidential Secretariat. "A Strategic Approach to Digitize Government Services." *President's Office*, November 13, 2024. https://www.presidentsoffice.gov.lk/a-strategic-approach-to-digitize-government-services/.

Presidential Secretariat. "PSGPACircular." January 13, 2020. https://www.presidentsoffice.gov.lk/wp-content/uploads/2020/01/PS_GPA_Cicular_01_2020.PDF.

Presidential Secretariat, Sri Lanka. "Use of Electronic Documents and Electronic Communication for Official Use." October 9, 2013. https://www.icta.lk/icta-assets/uploads/2016/03/Circular-Use-of-Electronic-Documents-and-Electronic-Communication-for-Official-Use_English1.pdf.

Public Access To Government Documents Gazette English (1980). https://archives.gov.lk/resources/215/Public%20Access%20To%20Government%20Documents%20Gazette%20English.pdf.

Raisa Wickrematunga v. Telecommunications Regulatory Commission of Sri Lanka (TRCSL), 106/2018 (2018). https://www.rticommission.lk/web/images/pdf/31032018/raisa-W.pdf.

Rajapakse, Chiranthi. "Comments on the Cyber Security Bill - Sri Lanka 2023." LIRNEasia, 2023. https://lirneasia.net/2023/08/comments-on-the-cyber-security-bill-sri-lanka-2023/.

Regulations Promulgated Under the Right to Information Act, No. 12 of 2016 (2017).

Right to Information Act, No. 12 of 2016 (2016). https://web.archive.org/web/20211222074002/http://rti.gov.lk/images/resources/RTI_Act_Sri_Lanka_E.pdf.

RTI Commission of Sri Lanka. *Selected Orders of the Right to Information Commission of Sri Lanka 2017-2018*. 2019. http://www.rticommission.lk/web/images/pdf/books/rtic-orders-2017-2018.pdf.

Samarajiva, Rohan. *Digitalisation Will Fail, Unless | Daily FT*. August 11, 24AD. https://www.ft.lk/columns/Digitalisation-will-fail-unless/4-768977.

Sooriyagoda, Lakmal. "Speaker's Act of Certifying Online Safety Bill Challenged in SC by Sumanthiran." *Daily Mirror*, February 16, 2024. https://www.dailymirror.lk/breaking-news/Speakers-act-of-certifying-Online-Safety-Bill-challenged-in-SC-by-Sumanthiran/108-277130.

"Sri Lanka - OpenStreetMap Wiki." Accessed July 16, 2024. https://wiki.openstreetmap.org/wiki/Sri_Lanka.

Sri Lanka CERT. "Proposed Information Security Policy Framework for Government Organizations." OnlineSafety.LK. Accessed August 7, 2023. https://www.onlinesafety.lk/government/.

"Sri Lanka Leader to Appoints Panel to Amend Flaws Anti-Corruption Law." Business. *EconomyNext*, 6:01 pm,Tuesday December 31, 2024. https://economynext.com/sri-lanka-leader-to-appoints-panel-to-amend-flaws-anti-corruption-law-197126.

"Sri Lanka: Proposed Online Safety Bill Would Be an Assault on Freedom of Expression, Opinion, and Information." Press Releases. *International Commission of Jurists*, September 29, 2023. https://www.icj.org/sri-lanka-proposed-online-safety-bill-would-be-an-assault-on-freedom-of-expression-opinion-and-information/.

Supreme Court Sri Lanka Broadcasting Authority Bill (1997). http://www.mediareform.lk/wp-content/uploads/2020/02/89-Sri-Lanka-Broadcasting-Authority-Bill-1997.pdf.

Survey Act English (2002). https://www.survey.gov.lk/sdweb/pdf/surveydocuments/Survey%20Act/Survey%20Act%20English.pdf.

"Table of RTIC Decisions." 2020. https://www.rticommission.lk/web/images/pdf/SDG/TABLE-OF-RTIC-DECISIONS-CLASSIFIED-AS-PER-UN-SDGS-582-2020.pdf.

The Copyright (Amendment) Act, Pub. L. Act No. 27 of 2012 (2012). https://www.wipo.int/wipolex/en/text/304385.

"The Department." Accessed January 9, 2024. https://www.survey.gov.lk/sdweb/page_content_about_us.php?id=8b8450664ade43f34efbc32a73059fdab247679f.

The Morning. "Data Protection Bill Further Delayed." January 18, 2020. https://themorning.lk//articles/66751.

The Personal Data Protection Bill, 2019, 373 of 2019 (2019).

The Sunday Times Sri Lanka. "Google 'Maps' Launches SL Project to Show People Shops, Where They Live." December 14, 2014. http://www.sundaytimes.lk/141214/business-times/google-maps-launches-sl-project-to-show-people-shops-where-they-live-131976.html.

Times Online. "Sri Lanka loses its membership of the Open Government Partnership." 2025. https://sundaytimes.lk/online/news-online/Sri-Lanka-loses-its-membership-of-the-Open-Government-Partnership/2-1149444.

Transparency International Sri Lanka v Presidential Secretariat (2017). https://www.rticommission.lk/web/images/pdf/rticappeal-005-006-2017/rtic-006-2017-en-06122018.pdf.

Verite Research. *Proactive Disclosure Under the RTI Act in Sri Lanka: Ranking Public Authorities 2023*. 2023. https://www.veriteresearch.org/wp-content/uploads/2023/09/20230904_ProactiveDisclosureReport_F_AM-1.pdf.

Walpola, Thilina. *"Implementation of Personal Data Protection Act Likely to Be Hampered by Political Interference"*. February 9, 2024. http://island.lk/implementation-of-personal-data-protection-act-likely-to-be-hampered-by-political-interference/.

Weerasinghe, Tharushi. "The New Digital ID to Be an Integrated e-NIC/MOSIP Solution." *The Sunday Times, Sri Lanka*, August 24, 2025. https://www.sundaytimes.lk/250824/news/the-new-digital-id-to-be-an-integrated-e-nicmosip-solution-609822.html.

Wickrematunge, Raisa. "Blocked: RTI Requests Reveal Process Behind Blocking of Websites in Sri Lanka." *Groundviews*, December 8, 2017. https://groundviews.org/2017/12/08/blocked-rti-requests-reveal-process-behind-blocking-of-websites-in-sri-lanka/.