

PERSONAL DATA PROTECTION ACT

NO: 09 OF 2022

What is the Personal Data Protection Act?	<p>Sri Lanka welcomed the Personal Data Protection Act No. 09 of 2022 (the “Act”) in March 2022 which provides for mechanisms of protecting of personal data, while simultaneously facilitating the growth and innovation in the digital economy in Sri Lanka with due protection being ensured to those identified as data subjects. The Act also intends strengthening cross-border co-operation while assuring the interoperability among personal data protection frameworks.</p> <p>The Act defines measures to protect personal data of individuals held by the government entities, banks, telecom operators, hospitals and other public and private personal data aggregating and processing entities.</p>
Why is the Personal Data Protection Act important to Sri Lanka?	<p>A personal data protection law became necessary in view of the digital strategies adopted by the government and private sector. In the context of contact tracing solutions for effective management of Covid-19 by health authorities and to further the digital identity initiative of Sri Lanka, this Act is of paramount importance, as it will strengthen the governance and administration of personal data.</p> <p>The Act is designed to balance the interest of the enterprises and organizations as against the rights of individuals to ensure transparency and accountability in data processing activities. The Act has imposed several obligations on those who collect and process personal data (the Act identifies and defines them as “Controllers” and “Processors” respectively). An entirely new set of statutory rights have been given to natural persons/individuals (referred to and defined as “Data Subjects”) under this Bill, and these are now known as “rights of data subjects”.</p> <p>A personal data protection law acts as a catalyst to attract investment in BPO/BPM and other data processing industries. As a result, this legislation has been given priority by the government, through the Ministry of Technology, to ensure cross governmental implementation.</p>
What standards were considered in	<p>During the various drafting stages of this Act, the drafting committee considered international best practices, such as the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, the Asia-Pacific</p>

<p>the drafting of this Act?</p>	<p>Economic Co-operation (APEC) Privacy Framework, Council of Europe Data Protection Convention, European Union (EU) General Data Protection Regulations (GDPR), and laws enacted in other jurisdictions such as the United Kingdom, Singapore, Australia and Mauritius, the State of California as well as the Indian Draft Bill on data protection.</p>
<p>What processes were followed in the drafting of this Act?</p>	<p>The considerations and conversations surrounding the drafting this Act have been vast and various, with engagement of stakeholders at various stages of the drafting process.</p> <p>This Act was formulated by a joint expert drafting committee represented by both public and private sectors, chaired by ICTA General Counsel, and the process was initiated by the then Ministry of Digital Infrastructure in February 2019. The Committee finalized a framework containing the proposals for a proposed data protection legislation, first published in June 2019. Consequently, there were seven (7) rounds of public stakeholder consultations and the committee received over 30 written submissions from individual experts, multinational corporations, international entities and domestic organizations, including the Right to Information Commission. Based on this feedback, draft of the Bill was prepared by the Legal Draftsman's Department on 16th September 2019 and thereafter on 3rd October 2019. The latter version was presented to Cabinet of Ministers and approval was granted in principle to proceed with next steps.</p> <p>Thereafter, Hon. Attorney General and team reviewed the draft over a period of 18 months, and provided observations on three (3) occasions, resulting in several version changes during 2020-21 period. During this period there were further stakeholder facilitated by Ceylon Chamber Commerce, Ministry of Justice, the Central Bank and TRCSL. Even after the Certificate of Constitutionality was issued on 25th June 2021, several domestic and international entities submitted observations to Secretary to the Ministry, including submissions from TISL and these were considered when formulating Committee stage amendments to the Bill.</p> <p>The work of the drafting committee was reviewed by an Independent Review Panel, co-chaired by former Supreme Court Justice K. T. Chitrasiri and former Vice Chancellor of the University of Colombo and Professor of Law, Prof. Savithri Goonesekera.</p>

<p>To whom does this Act apply?</p>	<p>The Act is designed to apply to entities located in Sri Lanka as well as outside Sri Lanka, including those offering goods or services to Sri Lankans and specifically targets data subjects in Sri Lanka. This may include digital platforms providing services to Sri Lankans from outside Sri Lanka. The Act, amongst other things, now provides for a legal framework to provide for mechanisms for the protection of personal data of Data Subjects (defined in the Act under Section 56).</p> <p>The Act requires Controllers to process data lawfully, in compliance with obligations for processing in Part I of the Act (see Section 5 to 12). Controllers implementing “a data protection management programme” in accordance with Section 12 would be complying with the obligations under Sections 5, 6, 7, 8, 9, 10 and 11.</p> <p>The Act also provides a range of rights to Data Subjects, referred to as “rights of data subjects” under Part II. The Data Subjects are guaranteed the right to withdraw consent if processing of the data is based on consent, right to object to processing of their data, right of access and rectification, right to erasure and request review of automated decision-making subject to certain conditions. However, it should be noted that Controllers have the right to grant or refuse or the requests subject to criteria specified in the Act.</p>
<p>Joint Declaration with the European Union (EU)</p>	<p>On 22nd February 2022, a Joint Declaration was released by the European Union, Australia, Comoros, India, Japan, Mauritius, New Zealand, the Republic of Korea, Singapore, Sri Lanka on privacy and the protection of personal data.</p> <p>The Signatory Nations, of which Sri Lanka is one, share a common vision of a human-centric approach to building trust with regard to the use of personal data, to fully embrace and realize the benefits of the digital revolution, which in turn would particularly help with achieving the UN 2030 Agenda for Sustainable Development.</p> <p>Building trust in how data is handled is key and it then encourages diverse societies and economies, individuals and communities, to adopt new technologies, and provide mechanisms for public authorities to be more open to sharing personal data with foreign partners and for commercial exchanges.</p> <p>The Declaration promotes this transformation and expects that the effective protection of personal data will play a crucial role and be a key enabler for cross-border cooperation.</p>

The Nations to the Joint Declaration hope to achieve this goal by fostering international cooperation to promote high levels of data protection and privacy standards based on certain core elements increasingly shared across the Indo-Pacific region, Europe and beyond.

Some core elements are:

- Comprehensive legal frameworks and policies covering both the private and public sectors;
- Core principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, limited data retention, data security and accountability;
- Enforceable rights of individuals, such as access, rectification, deletion, and safeguards with respect to automated decision-making such as transparency and the possibility to challenge the outcome;
- Safeguards for international transfers to enable cross-border data flows by ensuring that the protection travels with the data;
- Independent oversight by a dedicated supervisory authority and effective redress.

Being a signatory to this Declaration is important for Sri Lanka, which has now enacted its first Personal Data Protection legislation, as it clearly states its understanding of coexisting in a world where data moves easily between jurisdictions, thus ensuring interoperability promoting close cooperation between countries, in compliance with the relevant applicable legal frameworks, among supervisory authorities.