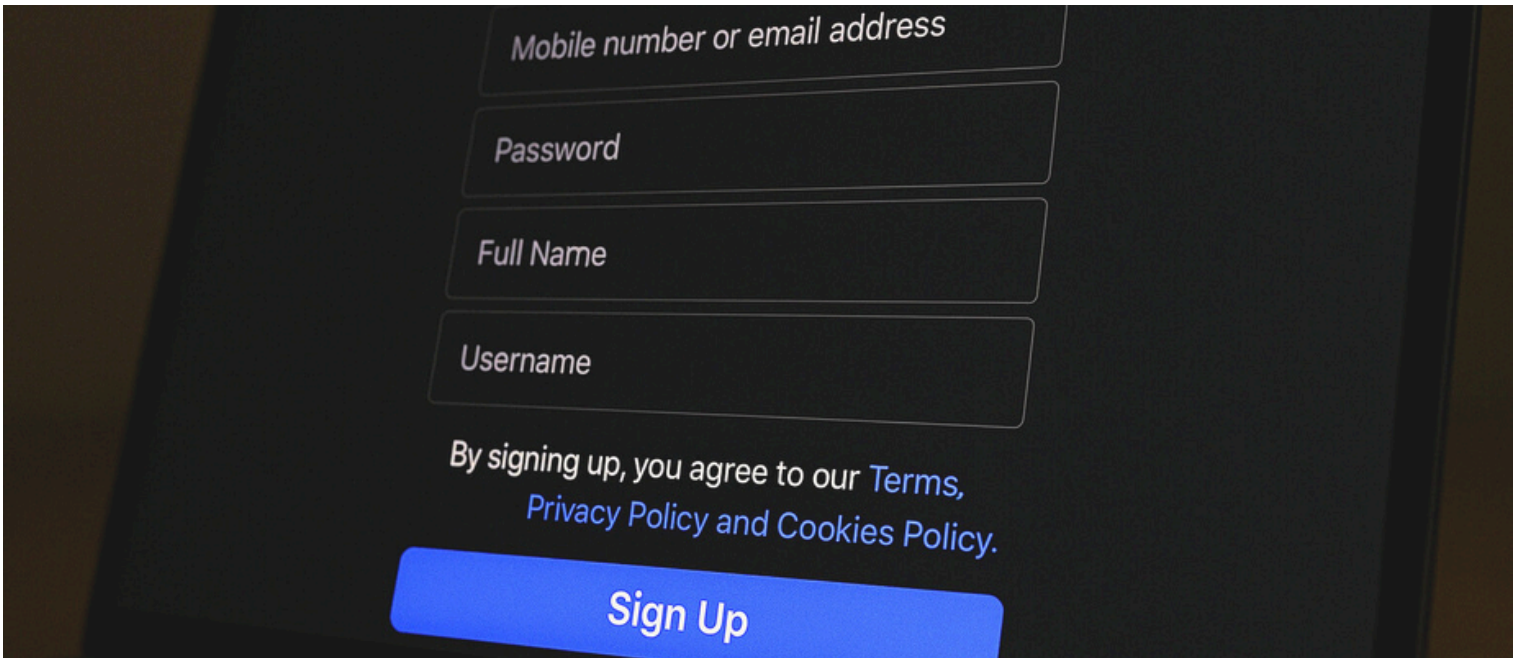

E–ALERT: PERSONAL DATA PROTECTION (AMENDMENT) ACT, NO. 22 OF 2025

Sudath Perera Associates

November 2025

BACKGROUND

The Personal Data Protection Act, No. 9 of 2022 ("**PDPA**") established Sri Lanka's first comprehensive data protection regime, setting out key obligations for data controllers and processors, recognizing rights for data subjects, and establishing the Data Protection Authority ("**DPA**") as the regulatory body.

The substantive provisions of the PDPA had been scheduled to come into operation on 18 March 2025 under Gazette No. 2366/08. However, in February 2025 the Ministry of Digital Economy announced that the Government would first introduce amendments to the PDPA, following consultations with the Data Protection Authority and the Legal Draftsman's Department. The Ministry noted that several adjustments were required to address practical implementation and public-sector readiness, particularly across ministries, provincial councils, local authorities and other government bodies, before the enforcement framework could take effect [1]. Accordingly, the general commencement of the PDPA was deferred pending enactment of the Amendment Bill.

Against this backdrop, the Personal Data Protection (Amendment) Act, No. 22 of 2025 ("**Amendment Act**") has been enacted on 30th October 2025, and introduces a series of targeted reforms designed to provide greater flexibility in the PDPA's operationalisation and to refine several of its core compliance obligations. The amendments address commencement timelines, streamline the exercise of data subject rights, refine the criteria for appointing Data Protection Officers ("**DPOs**"), and adjust requirements relating to Personal Data Protection Impact Assessments ("**PDPIAs**"). The Amendment Act also replaces the original cross-border data transfer mechanism with a more adaptable, safeguards-based framework to be implemented through directives issued by the DPA.

This e-alert examines the principal changes introduced by the Amendment Act and their impact on the compliance obligations of controllers and processors.

[1] https://www.dpa.gov.lk/newministry.php

COMMENCEMENT AND TIMELINES

Originally, all provisions of the PDPA, except Part IV (use of personal data to disseminate solicited messages) and Part V (establishment of the DPA), were to come into operation on a date appointed by the Minister, not earlier than eighteen months and not later than thirty-six months from the date the Speaker's certificate was endorsed [2]. Part IV was to come into operation between twenty-four and forty-eight months, while Part V was to take effect on a date appointed by the Minister, no later than the date fixed for the other provisions.

The Amendment Act removes these fixed timelines and instead allows the Minister to bring different Parts of the PDPA (other than section 1) into operation on such date or dates as may be specified by Order published in the Gazette. It also validates any actions already taken under Parts V, VI, VIII, IX, and X that were brought into force under the previous provisions.

GUIDELINES ISSUED BY THE DATA PROTECTION AUTHORITY

Section 12(2) of the PDPA, which previously allowed the DPA to issue guidelines specifically for Data Protection Management Programmes ("**DPMP"**), has been repealed. A new section 51A has been introduced, granting the DPA broader authority to issue guidelines on any matter under the PDPA, including those relating to DPMPs.

DATA SUBJECT RIGHTS

While the substantive rights of data subjects under the PDPA remain unchanged, the Amendment Act introduces important procedural amendments governing the manner in which such rights are to be exercised and enforced.

Extended scope of requests

Section 17, which sets out how controllers must respond to data subject requests, has been expanded to cover requests relating to automated individual decision-making. As a result, controllers are now required to respond to requests made by data subjects under sections 13 (right of access), 14 (right to withdrawal of consent and the right to request to refrain from further processing), 15 (right to rectification or completion), 16 (right to erasure), and 18 (right to review automated decisions).

Revised response timelines

The response period for data subject requests has been extended from twenty-one working days to one month from the date of the request, with the possibility of an additional two-month extension, provided that it does not exceed three months from the date of receipt of the request, and the data subject is informed of such an extension and the reasons for it.

Requests to be complied with free of charge

Controllers may no longer charge fees for responding to data subject requests, except in circumstances prescribed by the DPA.

Expanded rights to challenge automated decisions

Section 18 has been amended to extend the right of a data subject to challenge an automated decision that affects not only their rights under written law but also their constitutional rights.

[2] Which was determined as 18th March 2025, as per gazette notification 2366/08 dated 8th January 2024.

Broadened right of appeal

Section 19 has been amended to expand the right of appeal available to data subjects. Previously, appeals were limited to refusals to rectify, erase, refrain from further processing personal data, refusals of requests under section 17, or refusals to review automated decisions. The amended section now allows data subjects to appeal against refusals of access to personal data (under section 13) and refusals to withdraw consent (under section 14(1)).

DATA PROTECTION OFFICER

Section 20 of the PDPA originally required controllers or processors to appoint a DPO in the following cases:

Section 20(1)(a)- where processing was carried out by a ministry, government department, or public corporation (other than the judiciary in its judicial capacity); or

Section 20(1)(b)- where the controller's or processor's core activities involved:

i. a regular, and systematic monitoring of data subjects on a prescribed scale and magnitude;

ii. the processing special categories of personal data on a prescribed scale and magnitude; or

iii. processing which results in a risk of harm affecting the rights of the data subjects based on the nature and processing and its impact on data subjects.

Section 20(1)(a) has been amended so that public corporations are no longer automatically required to appoint a DPO, this obligation now applies only to ministries and government departments. Furthermore, the "risk of harm" criteria set out in Section 20(1)(b)(iii) has been amended to grant the DPA the discretion to determine this risk through guidelines issued under the PDPA. Instead of each controller assessing risk independently, the DPA will now specify, by way of guidelines, the categories of processing that trigger a mandatory DPO appointment.

Furthermore, under Section 20(5)(b) the DPO was responsible for "ensuring" compliance with the PDPA on behalf of the controller or processor. However, under the Amendment Act, the DPO's role has been redefined to focus on advising the controller or processor regarding their obligations and guiding them on how to comply with the PDPA, rather than being responsible for guaranteeing compliance.

The Amendment Act has also broadened the definition of a DPO to include third parties who are not directly employed by a controller or processor but who perform the responsibilities of a DPO under section 20(5). This amendment formally allows organizations to outsource the DPO function, for example to an external consultant or service provider.

PERSONAL DATA PROTECTION IMPACT ASSESSMENTS

Previously, section 24(5) of the PDPA required controllers to submit completed PDPIAs to the DPA. The Amendment Act now requires submission only upon a written request from the DPA.

Under section 25 of the PDPA, controllers were required to take measures to mitigate any risks of harm to data subjects identified through a PDPIA. The section also provided for consultation with the DPA where such risks could not be fully mitigated, allowing the DPA to issue instructions or require additional safeguards.

The Amendment Act narrows this framework in two ways. First, it limits the risk assessment obligation to risks arising under the PDPA itself, removing references to risks under other written laws. Second, it repeals subsections (2), (3), (4), (5), and (6), thereby removing the general consultation procedure and the DPA's power to issue binding directions following such consultation.

However, subsection (7) remains in effect and continues to require consultation with the DPA where the processing relates to national security, public order, or public health.

CROSS-BORDER DATA TRANSFERS

Under section 26 of the PDPA, cross-border data transfers were regulated through an "adequacy decision" mechanism. The Minister, in consultation with the DPA, could determine whether a third country provided an adequate level of protection for personal data. Transfers were permitted only to such approved countries or where appropriate safeguards were in place, with limited exceptions such as consent, contractual necessity, public interest, or emergencies. Public authorities were generally restricted from transferring personal data outside Sri Lanka except under an adequacy decision.

The Amendment Act repeals and replaces section 26, removing the concept of adequacy decisions in its entirety. The new provision adopts a more flexible approach, allowing controllers and processors (including public authorities) to engage in cross-border data flows provided they comply with the core provisions of the PDPA (Parts I and II and sections 20 to 25) and implement safeguards specified by directives issued by the DPA. These safeguards may take the form of contractual clauses or other binding instruments ensuring enforceable rights and remedies for data subjects.

While the adequacy decision process has been removed, but the PDPA continues to recognise limited grounds for transfer, such as explicit consent, the performance of a contract, the establishment or defence of legal claims, public interest, or emergencies affecting life or safety. The amended section provides that the transit of personal data through Sri Lanka is also permitted.

However, public authorities remain subject to stricter requirements and may transfer personal data to third countries only in respect of categories of data prescribed by the Minister on the recommendation of the DPA and in consultation with the relevant regulatory bodies.

The definition of "public authority" has been narrowed. While the PDPA previously included statutory bodies and institutions established by law, the amended definition limits it to Ministries, Departments, Provincial Councils, local authorities, and Ministries or Departments of Provincial Councils, expressly excluding public corporations and companies incorporated under the Companies Act No.07 of 2007.

Additionally, the definition of "third country" now broadly refers to any country or territory outside Sri Lanka.

TIMEFRAME FOR MAKING RULES

Under the PDPA, the DPA was required to make its first set of rules under section 52(1) within twenty-four months of Part V coming into operation (Part V establishes the Authority). As Part V came into effect on 17 July 2023, the original deadline would have fallen in July 2025.

The amendment extends this period to thirty-six months, giving the Authority until July 2026 to issue its first set of rules.

FOR FURTHER INFORMATION, PLEASE CONTACT:

Dushyantha Perera
Partner – Head of Corporate & Commercial Law
E: dushyantha@sudathpereraassociates.com
T: +94 11 7559944

Vashni Ekanayake
Senior Legal Assistant (Corporate & Commercial Law)
E: vashni@sudathpereraassociates.com
T: +94 11 7559944

Nishadhi Thilakaratne
Legal Assistant (Corporate & Commercial Law)
E: nishadhi@sudathpereraassociates.com
T: +94 11 7559944

Sudath Perera Associates is a leading independent law firm based in Sri Lanka. Further information about the firm can be obtained on its website – www.sudathpereraassociates.com

Sudath Perera Associates