# Digital Assets and Service Providers Act (DASPA) 2025

An Act to regulate providers of services relating to digital assets; to protect clients; to ensure market integrity; and for connected purposes.

URL: https://example.org/law/daspa-2025

# Table of Contents

# 1 General Provisions

1.1 Scope This Act applies to Digital Asset Service Providers ("DASPs") that conduct activities for or on behalf of clients within the jurisdiction, including custody, exchange, transfer, advisory, and issuance-related services.

1.2 Definitions "Digital Asset" means a digitally represented value or right that can be transferred or stored using distributed ledger or similar technology, whether or not it qualifies as a financial instrument under other laws. "Client" means any natural or legal person receiving services from a DASP.

1.3 Territorial Application This Act applies to DASPs established in the jurisdiction and to foreign DASPs that actively market to, or serve, clients located in the jurisdiction.

1.4 Interpretation In interpreting this Act, regard shall be had to its purpose of consumer protection, market integrity, and financial stability. Terms not defined herein shall be given their ordinary meaning in regulatory practice.

## 2 Authorization of Providers

2.1 Licensing Requirement No person shall provide in-scope services unless authorized as a DASP by the Competent Authority. Authorization shall be activity-based and limited to the services specified in the authorization decision.

2.2 Conditions for Authorization Applicants shall demonstrate: (a) fitness and propriety of controllers and key personnel; (b) adequate capitalization commensurate with scale and complexity; (c) sound governance with clear segregation of duties; (d) effective risk management, including cyber and operational risk controls; and (e) robust arrangements for safeguarding client assets.

2.3 Ongoing Obligations Authorized DASPs shall maintain: (1) accurate books and records; (2) effective internal controls and independent compliance; (3) incident reporting procedures; (4) policies for conflicts of interest; and (5) business continuity and disaster recovery plans.

2.4 Revocation and Suspension The Competent Authority may revoke or suspend authorization where the DASP: (i) breaches material provisions of this Act; (ii) no longer meets authorization conditions; (iii) provides misleading information; or (iv) fails to remedy deficiencies within the period specified by the Competent Authority.

## 3 Conduct of Business and Supervision

3.1 Client Asset Safeguarding DASPs shall segregate client assets from the DASP’s own assets and hold them in trust or a functionally equivalent legal arrangement. Rehypothecation of client assets is prohibited unless expressly permitted by written client consent and applicable law.

3.2 Disclosure and Transparency DASPs shall provide clear, fair, and not misleading information regarding risks, fees, and service conditions. Pre-contractual disclosures shall include custody arrangements, security practices, and dispute resolution options.

3.3 Marketing Communications Marketing shall be clearly identifiable as such and shall not downplay risks inherent in digital assets or overstate potential returns. Influencer-based promotions fall within the scope of this provision.

3.4 Operational Resilience DASPs shall implement appropriate measures to ensure continuity of critical services, including regular penetration testing, incident response runbooks, and post-incident learning reviews.

3.5 Outsourcing Material outsourcing shall follow a written policy, due diligence of service providers, and contractual rights that ensure access, audit, and termination for cause. The DASP remains fully responsible for outsourced functions.

3.6 Complaints Handling and Redress DASPs shall maintain prompt and effective complaints procedures and provide clients with access to independent alternative dispute resolution where available. Records of complaints and outcomes shall be retained for no less than seven years.

## 4 Enforcement, Sanctions, and Transitional Measures

4.1 Supervisory Powers The Competent Authority may conduct on-site and off-site inspections, require information, and issue binding directions to remedy identified deficiencies.

4.2 Administrative Sanctions Where a breach is established, the Competent Authority may impose administrative fines, public statements, and orders to cease or desist. In setting sanctions, the Authority shall consider gravity, duration, and cooperation.

4.3 Criminal Offences Knowingly providing in-scope services without authorization or falsifying records required under this Act constitutes a criminal offence punishable as prescribed by law.

4.4 Transitional Measures Persons providing in-scope services on the date of entry into force shall notify the Competent Authority within 90 days and may continue operations for up to 12 months, subject to good-faith progress toward authorization.

4.5 Entry into Force This Act shall enter into force on 1 October 2025.