The Personal Data Protection Act 2012

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

Scope and obligations

The Act applies to every organisation that collects, uses or discloses personal data in Singapore. Public agencies and individuals acting in a personal capacity are excepted.[1] Personal data is data about an individual who can be identified from that data or from that data together with other information to which the organisation has or is likely to have access. The obligations are grouped under headings that have become standard in Singapore compliance practice: consent, purpose limitation, notification, access and correction, accuracy, protection, retention limitation, transfer limitation, data breach notification and accountability.[2] The 2020 amendments, in force from 1 February 2021, added mandatory breach notification, a deemed-consent-by-notification mechanism and a legitimate-interests exception. They also raised the maximum financial penalty to 10 per cent of an organisation's annual turnover in Singapore where that turnover exceeds S$ 10 million. The higher penalties took effect on 1 October 2022.[3]

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

A licensed digital payment token service provider holds a great deal of personal data. It collects identity documents, addresses, source-of-funds evidence, device and IP data, transaction histories and wallet addresses. Each item is personal data. The Act requires the provider to notify its purposes, obtain consent or rely on an exception, protect the data with reasonable security arrangements and delete it when no longer needed for a legal or business purpose. The Personal Data Protection Commission has fined financial-sector organisations for inadequate protection following breaches, and crypto platforms are an obvious target for attackers who want the identity documents of people known to hold crypto assets.

Breach notification

An organisation that has reason to believe a data breach has occurred must assess it expeditiously. If the breach is notifiable, it must inform the Commission within three calendar days of that assessment and the affected individuals as soon as practicable. A breach is notifiable if it results or is likely to result in significant harm to the individuals or if it affects 500 or more individuals.[4] For a crypto platform, a leak of customer identity data is almost always notifiable, because the data can be used to target customers with phishing and physical coercion. A breach of the platform's hot wallet that does not expose personal data is not a data breach under the Act, although it will engage the MAS incident-reporting requirements under the Technology Risk Management Notice.[5]

Notes

1. Personal Data Protection Act 2012, ss 2 (definitions) and 4 (application). ↩
2. Personal Data Protection Act 2012, Parts 3 to 6B, in particular ss 13 (consent), 18 (purpose limitation), 20 (notification), 21–22 (access and correction), 23 (accuracy), 24 (protection), 25 (retention limitation), 26 (transfer limitation) and 26A–26E (data breach notification). ↩

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

3. Personal Data Protection (Amendment) Act 2020, commenced in phases from 1 February 2021. The increased financial penalty under s 48J took effect on 1 October 2022. ↩
4. Personal Data Protection Act 2012, ss 26B–26D, and Personal Data Protection (Notification of Data Breaches) Regulations 2021. ↩
5. MAS Notice on Technology Risk Management, requiring notification of relevant incidents within one hour. Part K, Chapter II and Part L, Chapter VII cover the regulatory reporting duties. ↩

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice. Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com