Data, systems and the compliance stack

Dr Alexander Ressos, TEP
Of Counsel, KGP Legal LLC
Attorney-at-Law (Switzerland and Germany), Solicitor (England & Wales and Hong Kong)

A dual-hub group runs one technology stack and must satisfy two data-protection laws and two sets of regulatory technology requirements. The Swiss Federal Act on Data Protection of 2023 and Singapore's Personal Data Protection Act 2012 are compatible enough that a single policy satisfies both. Switzerland recognises Singapore as a jurisdiction with adequate protection for transfers. Singapore permits transfers to Switzerland under the transfer limitation obligation on the basis of contractual safeguards.[1] The regulatory technology requirements are heavier in Singapore. MAS's Technology Risk Management Guidelines and the Notice on Cyber Hygiene apply to every licensee. They require board-level accountability, penetration testing, incident reporting within one hour of discovery of a relevant incident and controls over privileged access, which for a custodian means controls over key management.[2] Switzerland's FINMA Circular 2023/1 on operational risks and resilience applies to banks and FinIA institutions and imposes comparable duties with less prescriptive detail.[3]

The economical answer is to build the compliance stack once to the Singapore standard and apply it group-wide. A group that meets MAS TRM meets FINMA's expectations for a non-bank institution with margin to spare. The same holds for anti-money-laundering controls. A group programme built to MAS Notice PSN02 satisfies the Swiss SRO regulations in all material respects. Part L, Chapter VIII, and Part F, Chapter VIII, explain the few points where the Swiss rules are stricter, chiefly the CHF 1,000 identification threshold for exchange transactions and the treatment of unhosted wallets under the travel rule.

Notes

1. Federal Act on Data Protection of 25 September 2020 (FADP; DSG), SR 235.1, Art. 16 and Annex 1 to the Data Protection Ordinance of 31 August 2022 (DSV), SR 235.11 (list of states with adequate protection, including Singapore); Personal Data Protection Act 2012 (2020 Rev. Ed.), s. 26 and Personal Data Protection Regulations 2021, reg. 10 to 12 (transfer limitation obligation). Part D, Chapter X, and Part J, Chapter IX.
2. MAS, Technology Risk Management Guidelines, January 2021; MAS Notice PSN05 on Technology Risk Management and Notice PSN06 on Cyber Hygiene for payment service providers (incident notification within one hour). Part L, Chapter VII.
3. FINMA Circular 2023/1, "Operational risks and resilience – banks", of 7 December 2022, in force 1 January 2024, margin nos 50 ff. (ICT risks) and 98 ff. (critical data). Part F, Chapter VIII.

Copyright © 2026 Dr Alexander Ressos, TEP – Of Counsel, KGP Legal LLC. SingaporeIQ is an information website and gives no legal advice. For Singapore law advice through KGP Legal LLC, please write to alexander.ressos@kgplegal.com.sg