Cross-border transfers

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

The Transfer Limitation Obligation

An organisation may transfer personal data outside Singapore only if it takes appropriate steps to ensure that the recipient is bound by legally enforceable obligations to provide a standard of protection comparable to the Act. The Personal Data Protection Regulations 2021 specify that such obligations may arise from law, contract, binding corporate rules or any other legally binding instrument. The Commission has recognised the ASEAN Model Contractual Clauses as a suitable contractual basis.[1] Transfers may also be made with the individual's consent after notification of the risks, or where necessary for the performance of a contract with the individual. A Singapore exchange that shares customer data with a group company in Zug for compliance review, with a Swiss custodian for onboarding, or with a cloud provider in Europe must have one of these bases in place.

The Swiss side

Switzerland's revised Federal Act on Data Protection (FADP, DSG) has been in force since 1 September 2023. It permits transfers abroad only to countries whose legislation the Federal Council has recognised as providing adequate protection, or where safeguards such as standard contractual clauses or binding corporate rules are in place.[2] Singapore is not on the Swiss adequacy list as of 30 June 2026. A Zug entity sending personal data to its Singapore affiliate must therefore rely on standard contractual clauses, which in practice means the EU Standard Contractual Clauses with the Swiss amendments recognised by the Federal Data Protection and Information Commissioner. The Singapore entity sending data to Switzerland has the easier task, since Swiss law provides comparable protection and a simple intra-group agreement incorporating the Singapore obligations suffices. Part D, Chapter X discusses the Swiss rules.

Checklist

A Swiss–Singapore crypto group should have the following data protection documents in place before sharing customer data across the border. - A data map identifying what personal data each entity holds, where it is stored, and which cloud and analytics vendors process it. - An intra-group data transfer agreement incorporating the EU Standard Contractual Clauses with Swiss amendments for transfers from Switzerland, and the ASEAN Model Contractual Clauses or equivalent for transfers from Singapore. - Privacy notices in each jurisdiction that disclose cross-border transfers, blockchain analytics vendors and the retention periods required by AML law. - A breach response plan that meets the three-day PDPC notification, the Swiss "as soon as possible" notification to the Commissioner,

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

and the one-hour MAS incident notification. - A data retention schedule reconciling the five-year AML retention requirement with the retention limitation obligation. - An on-chain data policy stating that no personal data is written to a public blockchain and that wallet-address linkages are stored off-chain under access control.

Notes

1. Personal Data Protection Act 2012, s 26, and Personal Data Protection Regulations 2021, regs 10–11 (transfer of personal data outside Singapore).
2. Art. 16–17 FADP (SR 235.1). The list of adequate countries is in Annex 1 to the Data Protection Ordinance (SR 235.11).

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