Wallet addresses and on-chain data as personal data

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

The regulator's position

The Commission published a guide on data protection considerations for blockchain design in July 2022. It takes three central positions. Data written to a blockchain is personal data if the individual can be identified from it in combination with other information. An organisation that writes personal data to a blockchain remains responsible for it as a data controller. Pseudonymised data such as a wallet address or a hashed identifier may still be personal data where the organisation or others can link it to an individual.[1] The guide recommends that personal data be kept off-chain with only hashes or references on-chain and that permissioned networks be used where the participants can be bound by contract. Organisations should assess whether their use of a public blockchain is consistent with the retention limitation and correction obligations before deploying.

© 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.

Consequences for exchanges and protocols

An exchange that knows the identity of the customer behind a wallet address holds personal data in that address. Every transaction the customer makes on-chain from that address, which is public, is therefore personal data in the exchange's hands. The exchange's disclosure of the link between address and identity is a disclosure of personal data requiring consent or an exception. The exceptions cover disclosure required by law, which includes disclosure under a court order of the kind made in *CLM v CLN* and disclosure to law enforcement, and disclosure necessary for an investigation or proceedings.[2] An exchange served with a disclosure order should comply and should not treat the Act as a reason to delay. An exchange asked informally by a claimant's lawyer for account-holder details should refuse, because no exception covers voluntary disclosure to a private party.

Protocols face a different problem. A developer who writes an identity attribute to a public chain, for instance a soulbound token recording that an address has passed verification, has created a permanent public record that cannot be corrected or deleted. The Commission's guidance treats this as a design failure unless the attribute cannot be linked to an individual. In practice the only safe design keeps identity off-chain and records on-chain nothing more than a cryptographic proof that a verification occurred.

Notes

1. Personal Data Protection Commission, *Guide on Personal Data Protection Considerations for Blockchain Design* (July 2022). ↩
2. Personal Data Protection Act 2012, First Schedule (exceptions to consent), including disclosure required or authorised by law and disclosure necessary for investigations or proceedings. ↩

© 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.

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