pdpc
PERSONAL DATA PROTECTION COMMISSION SINGAPORE

PROTECTING PERSONAL DATA ON BLOCKCHAINS

Developing a blockchain application that stores and processes personal data?

The PDPC's Guide on Personal Data Protection Considerations for Blockchain Design provides general guidance for designing blockchain applications. Here are some key takeaways from the Guide.

#1 ANTICIPATE POTENTIAL COMPLIANCE ISSUES WHEN PLANNING TO STORE PERSONAL DATA ON BLOCKCHAINS

As data stored on a blockchain is decentralised and tamper-resistant, this poses unique compliance issues under the Personal Data Protection Act (PDPA).

Decentralised

Data is replicated on multiple nodes, often across different jurisdictions

Tamper-resistant

Written data cannot be directly edited or deleted

Leads to compliance issues resulting from:

Accountability

Challenges in assigning data controllership over access, use and transfer of on-chain personal data, especially if node operators are unknown

Immutability

Challenges in complying with PDPA obligations to enable data correction or deletion, and ensure data protection in the long term

#2 DO NOT STORE ANY PERSONAL DATA ON-CHAIN ON A PERMISSIONLESS BLOCKCHAIN, WHETHER IN-CLEAR, ENCRYPTED OR ANONYMISED

In practice, it is difficult to protect and ensure accountability over personal data stored on a permissionless blockchain network. This is due to the anonymity of public nodes and lack of access controls. Therefore, personal data should not be stored on a permissionless blockchain whether in-clear, encrypted or anonymised, unless consent has been obtained from the individual for public disclosure.

#3 ENCRYPT OR ANONYMISE ALL PERSONAL DATA WRITTEN ON-CHAIN ON A PERMISSIONED BLOCKCHAIN

Access to personal data (encrypted or anonymised) should be provided only to authorised blockchain participants that have a business purpose to use the data. They must also be able to ensure adequate protection for the data.

Legally binding consortium agreements or contracts, with clear data controller or data intermediary obligations, should be enforced by blockchain operators on all participants to ensure PDPA compliance.

Technical measures, complemented by contractual and operational controls, should be implemented to enable the fulfilment of other PDPA obligations. These include:

- ***Protection obligations:***
  - Encrypt or anonymise personal data on-chain using industry-standard algorithms or practices; and
  - Allow only authorised participants to access the data with the decryption keys or identity matching tables provided through off-chain channels.
- ***Correction and retention limitation obligations:***
  - Enable data correction through insertion of new entries with encrypted corrected data; and
  - Mandate secure disposal of decryption keys of unneeded or erroneous data, rendering such data indecipherable.

#4 USE OFF-CHAIN APPROACHES TO FURTHER MITIGATE PERSONAL DATA PROTECTION RISKS ON PERMISSIONLESS OR PERMISSIONED BLOCKCHAINS

Application service providers should design their applications such that personal data is stored in an off-chain database or data repository where traditional access control mechanisms can be instituted.[1]

Only a hash of the personal data or a hash of the link to the off-chain database should be written on-chain.

- Ensure hashes generated are reasonably strong (e.g. by using industry-standard algorithms and incorporating a salt) to prevent attackers from using pre-computed tables to infer the hashed data. This is especially important for data that follows pre-determined formats, such as NRIC numbers.

[1] *Refer to PDPC's Guide on Data Protection Practices for ICT Systems for a compilation of data protection practices which organisations may incorporate into their off-chain systems.*

Supported by INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In support of SG:DIGITAL

Find out more at **www.pdpc.gov.sg/blockchain**