Singapore: PDPC publishes guide on personal data protection considerations for blockchain design

In brief

In July 2022, the Singapore Personal Data Protection Commission (PDPC) published a guide to help organisations comply with the Personal Data Protection Act (PDPA) when deploying blockchain applications that process personal data ("**Guide**"). Across the world, businesses and organisations are beginning to deploy blockchains in wide-ranging applications for finance and supply chain management. These applications may start storing personal data in these blockchain networks, which poses risks of noncompliance with the PDPA. As such, this Guide provides a broad set of principles and considerations for organisations to design their blockchain applications to be PDPA-compliant, thus ensuring more accountable management of customers' personal data.

In this issue

In more detail

While this Guide is not legally binding on individuals and organisations, it reflects the PDPC's stance with regard to the handling of personal data on blockchain networks. Organisations should look into and consider the best practices that are provided in the Guide to ensure that they are in compliance with their legal obligations under the PDPA and are not exposed to legal risks and liabilities.

Target Audience

The Guide is for the following organisations:

(a) Blockchain operators (i.e., those that govern, configure and operate blockchain networks and consortia)

(b) Application service providers (i.e., those that design, deploy and maintain applications on blockchain networks)

(c) Participating organisations (i.e., those that use blockchain applications)

While the Guide focuses on blockchain technology given its prevalence, some of the principles and recommendations here may be broadly applicable to Distributed Ledger Technologies (DLTs), depending on the nature of the DLT implementation.

Key terminology

- **DLT**: An umbrella term for a ledger shared across a set of DLT nodes and synchronised between DLT nodes using a consensus mechanism
- **Blockchain**: A specific sub-type of distributed ledger with confirmed blocks organised in an append-only, sequential chain using cryptographic links
- **Permissioned network**: A network containing a permissions layer that allows an entity or consortium of entities to set technical and contractual controls on: (a) who can join and participate in the network; and (b) what those entities can do on the network
- **Permissionless network**: A network without a permissions layer
- **On-chain personal data**: Personal data that is published on, or accessible via, a blockchain in cleartext

Associated roles

- **Blockchain operator**: An organisation responsible for the design, governance, configuration and operation of a permissioned blockchain network, application and service offered to participating organisations in the blockchain
- **Node operator**: An organisation that runs blockchain nodes that store copies of all blockchain data and are responsible for validating and reconciling the data
- **Application service provider (ASP)**: An organisation that operates an application on top of a blockchain network
- **Participating organisation**: An organisation that makes use of the services and functionalities in a permissionless or permissioned blockchain network

Personal data protection risks and considerations arising from blockchains

Accountability issues

In blockchain networks, data is stored in a decentralised fashion where copies of the ledger are hosted on multiple nodes in the network and which often exist across different jurisdictions. This leads to accountability issues in complying with PDPA obligations, giving rise to the following challenges:

Challenges	Description
Data controllership	• Under the PDPA, organisations need to set controls on who can access and use the personal data in their possession or control. • However, this may be difficult if the personal data is committed on-chain and the controls are dependent on the degree of oversight the organisations have over the blockchain participants and mode operators.
Transfer limitation obligation (TLO)	• The TLO requires personal data transferred overseas to be protected to a comparable standard to that under the PDPA. • Hence, if an organisation commits personal data on a blockchain with nodes spanning multiple jurisdictions, it has to ensure that these jurisdictions have comparable protections to comply with the TLO.
Consent and purpose limitation	• Under the PDPA, organisations are prohibited from collecting, using or disclosing an individual's personal data unless the individual gives, or is deemed to have given, consent for the collection, use or disclosure of their personal data for a specific purpose. • However, this may be difficult where data written on-chain is publicly accessible by all participants, making it impossible for organisations to effectively establish control over the collection, use and disclosure of the data by another participant.

Immutability issues

In blockchain networks, stored data is tamper-resistant since records that have been committed on the chain cannot be edited or deleted. This leads to immutability issues in complying with PDPA obligations, giving rise to the following challenges:

Challenges	Description
Protection obligation	For encrypted personal data stored on permissionless blockchain, the effectiveness of protection mechanisms (e.g., encryption) can be expected to degrade over time as threat actors' methods and computing power to break these mechanisms improve.
Retention limitation obligation	As the data committed on-chain is immutable, it cannot be erased or modified. Hence, for effective disposal, data would have to be committed on-chain in such a way that, post-disposal, it is rendered indecipherable by anyone that can access the data (e.g., encryption and disposal of the decryption key).

The degree to which accountability and immutability pose issues to blockchain participants differs based on whether the blockchain application is hosted on a permissionless or permissioned network.

Designing blockchain applications for PDPA compliance

(a) Considerations and recommendations for personal data on permissionless blockchain networks

Accountability and immutability issues pose a higher risk of noncompliance to the PDPA for organisations on a permissionless blockchain network.

Issues	Description	Measures
Accountability issues	• Any personal data that is committed on-chain is replicated on multiple nodes in the network, making the data publicly accessible to and usable by anyone participating in the permissionless network. • No operator controls participation in a permissionless network. Hence, it is impossible to assert data controllership or enforce any protection obligations on participants for personal data written on-chain. • It is impossible to control or know which jurisdictions the nodes of a permissionless network reside in, making it difficult for any responsible organisation to assess comparable protection for personal data written on-chain.	• ASPs building applications on permissionless blockchains should design their applications such that no personal data controlled by participating organisations is written on-chain either in cleartext, encrypted or anonymised forms. • Participating organisations should avoid business use cases that require uploading any personal data on-chain in cleartext, encrypted or anonymised forms onto a permissionless blockchain.
Immutability issues	• Data committed on-chain stays on it permanently as long as the blockchain network exists. • As long as there are operating nodes, threat actors will be able to access the publicly available data and: (a) conduct re-identification attacks; or (b) decrypt encrypted data uploaded on the blockchain.	

(b) Considerations and recommendations for personal data on permissioned blockchain networks

Permissioned blockchain networks typically have blockchain operators that can limit participation in the network to known and authorised participants. These participants are usually required to enter into a consortium agreement, which establishes a layer of contractual controls to complement technical controls. Hence, the operator helps to mitigate some of the accountability and immutability issues faced in permissionless networks through technical and contractual controls.

Issues	Description	Measures
Accountability issues	• While a permissioned blockchain network is only restricted to authorised participating organisations, any personal data written on-chain in cleartext will be accessible by all other participants that host or operate nodes. • Hence, all node operators are in possession of the data, thereby inadvertently increasing the regulatory burden on them.	• Any personal data written on-chain should be encrypted or anonymised, and access should only be provided to authorised participants with a business purpose for the data. • Blockchain operators should implement and effectively enforce legally binding consortium agreements to ensure PDPA compliance from participants with clear data controller or data intermediary obligations. • Blockchain operators should ensure that technical measures, complemented with contractual and operational controls, are implemented to enable the fulfilment of other PDPA obligations. • Blockchain operators should regularly review technical measures (e.g., encryption or other privacy preserving technologies).
Immutability issues	• As participation can be curated and controlled, the risk of an unknown threat actor decrypting encrypted data or re-identifying anonymised data on-chain is more manageable on permissioned blockchains. • Besides protecting the data, protection mechanisms such as encryption also help overcome immutability issues.	

(c) Using off-chain approaches to further mitigate personal data protection risks on permissionless or permissioned networks

Organisations that wish to process personal data as part of a blockchain application can consider off-chain approaches that store personal data in centralised data repositories, while only writing representations of the personal data on-chain.

The approach is as follows:

- ASPs 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.

- Only a hash of the personal data or a hash to the link to the off-chain database should be written on-chain. Any change in the underlying data will generate a completely different hash. This allows the hash to serve as an immutable verification of the underlying data's integrity, if written on-chain.
- Hashes generated should be reasonably strong to prevent attackers from using pre-computed tables to infer the data that is hashed.

Under this approach, the regulatory treatment of personal data is identical to that of traditional databases since the personal data is stored entirely off-chain. Blockchain participants can therefore use traditional industry-standard protection controls, policies and processes to ensure that the off-chain data is protected, and comparable data protection is in place when sharing data with participating organisations in different jurisdictions.

This approach can thus be used to fulfil personal data protection obligations in both permissionless and permissioned networks.

Other approaches under development

Apart from the above approach to off-chain storage, many permissionless networks are also building hybrid, layer-2 and other suitable solutions that allow data to be stored, processed or transacted off the main permissionless layer.

These emerging approaches include the following:

(a) Hybrid blockchain approaches that combine the use of a public permissionless chain with a private permissioned blockchain component that can be used to process transactions safely without exposure to the public blockchain

(b) Using solutions that process data and transactions on a private network layer built on top of a public permissionless chain, while only storing the proof or hash of data or transactions on the public permissionless layer (e.g., nested blockchains, state channels and zero-knowledge proofs)

Data protection management programme

Lastly, it is good practice for organisations, especially operators of blockchain consortia, to implement a Data Protection Management Programme (DPMP). As part of the DPMP, the blockchain operator should, where applicable, carry out the following:

(a) Establish an oversight committee for the blockchain consortium, where relevant.

(b) Ensure that the data protection officer of each participating organisation of the blockchain consortium oversees proper PDPA compliance through the policies and processes of the blockchain application within his or her own organisation and the consortium.

(c) Set policies and rules to determine the roles, responsibilities and rights of each participant in the blockchain application.

(d) Conduct a Data Protection Impact Assessment to identify and assess potential risks to personal data in the blockchain network and application.

(e) Regularly review the data protection and cybersecurity policies and processes put in place to ensure continued relevance in view of changes to technology, industry best practices and regulations.

The complete Guide on Personal Data Protection Considerations for Blockchain Design can be accessed here.

Contact Us

Andy Leck
Principal
Singapore
andy.leck@bakermckenzie.com

Ken Chia
Principal
Singapore
ken.chia@bakermckenzie.com

Lim Ren Jun
Principal
Singapore
ren.jun.lim@bakermckenzie.com

Alex Toh
Local Principal
Singapore
alex.toh@bakermckenzie.com

Abe Sun
Principal
Singapore
vasan.abe.sun@bakermckenzie.com