Technology, Media & Telecommunications

PDPC Launches Guide on Personal Data Protection Considerations for Blockchain Design

Introduction

On 18 July 2022, the Personal Data Protection Commission ("**PDPC**") launched the Guide on Personal Data Protection Considerations for Blockchain Design ("**Guide**") to help organisations with blockchain adoption.

The Guide provides principles and considerations on how to comply with the Personal Data Protection Act 2012 ("**PDPA**") when deploying blockchain applications that process personal data. It also provides guidance on data protection by design ("**DPbD**") considerations for organisations to implement more accountable management of customers' personal data. Specifically, it looks at:

1. Considerations and recommendations for personal data on **permissionless** blockchain networks;
2. Considerations and recommendations for personal data on **permissioned** blockchain networks; and
3. Using off-chain approaches to further mitigate personal data protection risks on both permissionless and permissioned networks.

In its Annex, it also covers developing a data protection management programme ("**DPMP**") for blockchain operators.

The Guide will be relevant to organisations that:

1. Govern, configure and operate blockchain networks and consortia (i.e. blockchain operators);
2. Design, deploy and maintain applications on blockchain networks (i.e. application service providers); and
3. Use blockchain applications (i.e. participating organisations).

In this Update, we elaborate on the key points of the Guide. Although largely focused on blockchain technology, some of the Guide's principles and recommendations may be applicable to other Distributed Ledger Technologies ("**DLTs**") as well.

Background and Limitations

"DLT" is an umbrella term for a "ledger shared across a set of DLT nodes and synchronised between DLT nodes using a consensus mechanism". The term "blockchain" refers to a specific sub-type of "distributed ledger with confirmed blocks organised in an append-only, sequential chain using cryptographic links".

Businesses and organisations across the world are starting to deploy DLTs in applications for finance and supply chain management. Some of these applications may store personal data in these blockchain networks.

While blockchains are a type of DLT, there are differences in how DLTs and blockchains store and transmit data relative to centralised systems. For organisations planning to adopt blockchain, the bulk of the data will still be stored and managed by traditional database management systems. Consequently, organisations may be unsure as to how blockchain applications can be designed in compliance with personal data protection obligations under the PDPA.

The Guide aims to help blockchain adoption by clarifying how to comply with the PDPA when deploying blockchain applications that process personal data.

PDPC has also published an infographic to summarise four broad takeaways from the Guide:

1. Anticipate potential compliance issues when planning to store personal data on blockchains.
2. Do not store any personal data on-chain on a permissionless blockchain, whether in-clear, encrypted or anonymised.
3. Encrypt or anonymise all personal data written on-chain on a permissioned blockchain.
4. Use off-chain approaches to further mitigate personal data protection risks on permissionless or permissioned blockchains.

Key Points

(A) Considerations and recommendations for permissionless blockchain networks

By way of background, the Guide classifies blockchain networks based on whether they contain a **permissions layer** that allows an entity or consortium of entities to set technical and contractual controls on: (i) who can join and participate in the network; and (ii) what those entities can do on the network.

Permissionless blockchain networks generally allow anyone (i.e. the public) to host nodes and read or write data on the network anonymously. Consequently, data written on-chain may be hosted on multiple nodes residing in various jurisdictions, and can be accessed by any entity that is participating in the permissionless network. As a result, accountability and immutability issues pose a higher risk of non-compliance with the PDPA.

PDPC considers any personal data published in-clear on a permissionless blockchain a form of public disclosure. Personal data should only be written on a permissionless blockchain if consent has been obtained from the individuals, or if the data is already publicly available.

The baseline recommendations are:

1. Application service providers ("**ASPs**") should design their applications such that no personal data controlled by participating organisations is written on-chain either in cleartext, encrypted or anonymised forms.

2. Similarly, 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.

(B) Considerations and recommendations for permissioned blockchain networks

In contrast with permissionless networks, permissioned blockchain networks typically have blockchain operators that can limit participation in the network to known and authorised participants. Participants are usually required to enter into a consortium agreement, which establishes a layer of contractual controls to complement technical controls, mitigating some of the accountability and immutability issues faced in permissionless networks.

The baseline recommendations are:

1. Any personal data written on-chain should be encrypted or anonymised, and access (e.g. decryption keys or identity mapping tables) should only be provided to authorised participants with a business purpose for the data.

2. Blockchain operators should implement and effectively enforce legally binding consortium agreements or contracts to ensure PDPA compliance from participants with clear data controller or data intermediary obligations.

3. Blockchain operators should ensure that technical measures, complemented by contractual and operational controls, are implemented to enable the fulfilment of other PDPA obligations (e.g. protection, correction and retention limitation obligations).

4. Blockchain operators should also regularly review these technical measures to ensure that industry-recognised standards, algorithms and practices are used; policies and processes are put in place to safely manage and protect the relevant keys (such as decryption and encryption keys); and that technological developments are monitored on an ongoing basis to ensure the protection measures remain relevant.

(C) Off-chain approaches to mitigate risks

Instead of writing personal data on-chain, organisations can consider off-chain approaches that store personal data in centralised data repositories, while only writing representations of the personal data on-chain.

This can be achieved through the following:

1. ASPs designing their applications such that personal data is stored in an off-chain database or data repository where traditional access control mechanisms can be instituted.
2. Only a hash of the personal data or a hash of the link to the off-chain database should be written on-chain. The hash can be used as a digital signature to immutably verify the integrity of the underlying data.
3. Hashes generated should be reasonably strong (e.g. use industry-standard algorithms and incorporate a salt) to prevent attackers from using pre-computed tables to infer the data that is hashed, especially data that follows pre-determined formats such as NRIC numbers.

(D) Developing a data protection management programme for blockchain operators

To foster awareness and accountability over personal data in all blockchain participants, a blockchain operator should implement a DPMP. The DPMP should include the following actions:

1. Establishing an oversight committee for the blockchain consortium where relevant;

2. Ensuring that the data protection officer of each consortium participant oversees proper PDPA compliance;

3. Setting policies and rules to determine the roles, responsibilities and rights of each participant in the blockchain application. Where possible, legally binding mechanisms should be used to get all participants to abide by these policies as a pre-condition for joining the network;

4. Conducting a Data Protection Impact Assessment (DPIA) to identify and assess potential risks to personal data in the blockchain network and application; and

5. Regularly reviewing data protection and cybersecurity policies and processes to ensure continued relevance in light of changes to technology, industry best practices and regulations.

Concluding Words

The Guide provides welcome guidance to organisations wishing to ensure that their blockchain applications will be in compliance with their PDPA obligations. It will continue to be updated and revised regularly, as it is intended to be a living document. However, organisations should note that its

recommendations do not ensure compliance with other data protection or privacy laws, such as the European Union General Data Privacy Regulations (GDPR).

For further queries, please feel free to contact our team below.

Contacts

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0786

steve.tan@rajahtann.com

Benjamin Cheong
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0738

benjamin.cheong@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications

T +65 6232 0752

lionel.tan@rajahtann.com

Tanya Tang
Partner (Chief Economic and Policy Advisor), Technology, Media & Telecommunications

T +65 6232 0298

tanya.tang@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com.

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

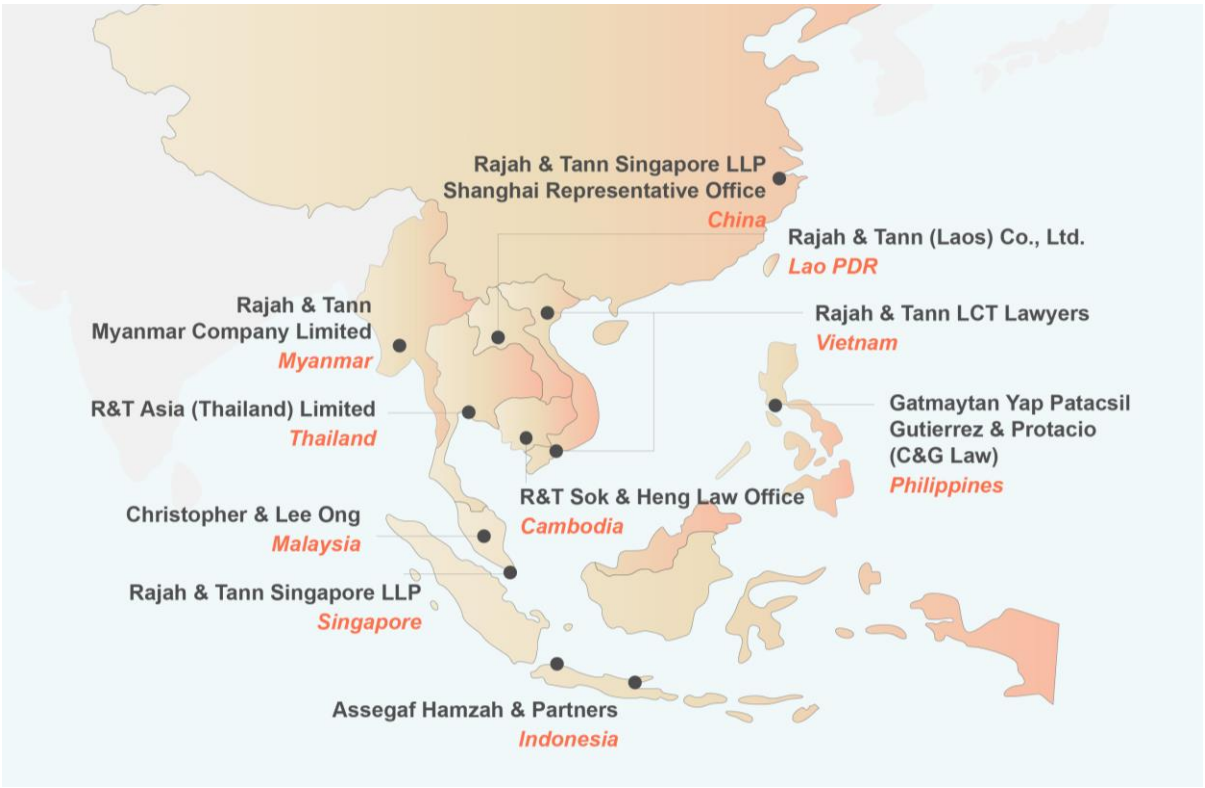
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.