pdpc

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

GUIDE ON

PERSONAL DATA PROTECTION CONSIDERATIONS FOR BLOCKCHAIN DESIGN

Supported by

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In support of

SG:DIGITAL

CONTENTS

PART I: OBJECTIVE, BACKGROUND AND CONTEXT

WHAT DOES THIS GUIDE ADDRESS?

Businesses and organisations across the world are starting to deploy Distributed Ledger Technologies ("**DLTs**"), such as blockchains, in wide-ranging applications for finance and supply chain management. Some of these applications may start storing personal data in these blockchain networks. However, due to differences in how blockchains and DLTs store and transmit data relative to centralised systems, organisations may be unsure as to how blockchain applications can be designed in compliance with personal data protection obligations under the Personal Data Protection Act ("**PDPA**").

This Guide aims to help blockchain adoption by clarifying how to comply with the PDPA when deploying blockchain applications that process personal data. It provides guidance on data protection by design ("**DPbD**") considerations for more accountable management of customers' personal data. This Guide is for organisations which:

A. Govern, configure and operate blockchain networks and consortia (i.e. blockchain operators);

B. Design, deploy and maintain applications on blockchain networks (i.e. application service providers); and

C. Use blockchain applications (i.e. participating organisations).

This Guide covers:

The policy considerations and risks associated with writing personal data on both permissionless and permissioned blockchains; and

Considerations for DPbD approaches with respect to the storage and transmission of personal data on blockchains.

Given the variety of blockchain types and approaches, this Guide does not attempt to be a comprehensive reference or prescribe specific implementations for blockchain applications. Instead, it provides organisations with a broad set of principles and considerations in designing and configuring their blockchain applications to be PDPA-compliant. While the focus of this Guide is on blockchain technology, given its prevalence, some of the principles and recommendations discussed here may be broadly applicable to DLTs as well, depending on the nature of the DLT implementation.

Additionally, the recommendations set out in this Guide do not ensure compliance with other data protection or privacy laws, such as the European Union ("**EU**") General Data Privacy Regulations ("**GDPR**").

Lastly, this Guide is intended to be a living document, and will be updated and revised regularly to ensure its recommendations remain relevant in the fast-changing blockchain industry.

BACKGROUND AND STARTING POINT

Blockchain technologies are typically deployed as part of a larger Information Technology ("**IT**") system, but do not replace the need for traditional transactional or relational databases to store data. Therefore, organisations planning to adopt blockchain should note that the bulk of data will still be stored and managed by traditional database management systems. They must then consider what subset of the data needs to be stored on the blockchain and make design choices over how the data may be stored to fulfil their business requirements. This document intends to guide organisations in making these choices when storing personal data on a blockchain network.

In addition to following the guidance set out in this document, it is good practice for organisations, especially operators of blockchain consortia, to implement a Data Protection Management Programme ("**DPMP**"). The DPMP establishes a robust data protection infrastructure within consortia and demonstrates that the consortia and their participants are accountable for their customers' personal data. (See the **Annex** for more details on the DPMP).

WHAT IS A BLOCKCHAIN AND WHAT ARE THE ASSOCIATED ROLES?

"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".[1] Given the prevalence of the blockchain model of distributed ledger, this Guide focuses on blockchain technologies for its policy analysis and recommendations.

The blockchain's key utility is that of a decentralised and tamper-resistant store of data that can act as a single, irrefutable source of truth without the need for a trusted centralised intermediary. This has enabled use cases such as document verification, digital asset storage and transfer and supply chain tracking, with these applications built on top of blockchain networks.

Permissionless vs Permissioned Networks

For the purposes of this Guide, we classify 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:

A. Who can join and participate in the network; and

B. What those entities can do on the network (e.g. what data they can write, use or disclose on that network).

Networks without such a permissions layer are known as **permissionless** networks, while those with such a permissions layer are known as **permissioned** networks. Both permissionless and permissioned networks have their own benefits, drawbacks and applicable use cases, and this Guide does not recommend the use of one over the other.

[1] *ISO/DIS 22739 – Terminology of Blockchain and Distributed Ledger Technologies. (3.6, 3.23)*

Roles in a Blockchain Network

An organisation can play multiple roles in a blockchain network. We can classify blockchain participants into four broad archetypes:

Blockchain operators (referred to as 'operators' in this Guide) refer to an organisation or a consortium of organisations responsible for the design, governance, configuration and operation of a **permissioned** blockchain network, application and service offered to participating organisations in the blockchain. The blockchain operator can also be a participating organisation using the services in the network or running its own application on the network (i.e. serving as an application service provider).

Node operators run blockchain nodes that store copies of all blockchain data and are responsible for validating and reconciling the data. In a permissionless network, any entity can run a node, while in a permissioned network, the blockchain operator determines which entities can run nodes. Nodes may be run by participating organisations or vendors contracted by a blockchain operator.

Application service providers ("**ASPs**") are organisations that operate an application on top of a blockchain network.

Participating organisations are organisations that make use of the services and functionalities in a permissionless or permissioned blockchain network.

Example: Roles of Organisations in a Permissionless Blockchain Network

OpenCerts is a blockchain platform developed by the Government Technology Agency of Singapore ("**GovTech**") in cooperation with the OpenCerts consortium. It offers an easy and reliable way for schools to issue and validate tamper-resistant digital academic certificates to students. As OpenCerts runs on the Ethereum permissionless blockchain, the participants may be classified as follows:

- **Blockchain operator** – none as it runs on a permissionless blockchain*.
- **Node operator** – any entity can participate as public node operator in the Ethereum permissionless blockchain.
- **ASP** – GovTech is the ASP operating and maintaining the OpenCerts platform.
- **Participating organisation** – any organisation (e.g. a company or an educational institution) can be a participating organisation of the Opencerts framework to issue and validate certificates.

**While the Ethereum community (i.e. anyone) can collectively propose changes to the design, governance and configuration of the network (which are subject to the approval of Ethereum protocol developers and node operators), no operator can control or restrict participation in the community or network.*

Example: Roles of Organisations in a Permissioned Blockchain Network

Contour is a trade finance network using Corda (a permissioned blockchain technology) to enable banks, partners and corporates to digitise and improve workflow management for trade finance products, such as letters of credit. Contour primarily offers this solution via a Software-as-a-Service ("**SaaS**") model, but also offers self-hosting options to clients. It maintains and operates the application, network and infrastructure for end users, which comprise major trade banks, global trading companies and small-to medium-sized enterprises. Its participants may be classified as follows:

- **Blockchain operator** – Contour is the business network operator governing access to the permissioned blockchain network.
- **Node operator** – Contour is the node operator for its SaaS clients, and participants authorised by Contour can also be their own node operators.
- **ASP** – Contour is also the ASP operating and maintaining the solution, including the application programming interfaces ("**APIs**") for partners to use.
- **Participating organisations** – banks, corporates and partners wanting to use the service need to sign up as members and adhere to Contour's terms and conditions.

WHAT PERSONAL DATA PROTECTION RISKS AND CONSIDERATIONS MIGHT ARISE WITH BLOCKCHAINS?

Blockchain networks differ from conventional databases in two key ways:

A **Data Is Stored in a Decentralised Fashion.** In a blockchain network, copies of the ledger are hosted on multiple nodes in the network which often exist across different jurisdictions. Addition of new data onto the chain must be validated and accepted by a majority of network nodes ("consensus"), after which the new data will be replicated across copies of the ledger within the network.

B **Stored Data Is Tamper-Resistant.** The blockchain is designed to be append-only, meaning that records that have been committed on the chain cannot be edited or deleted. This grants blockchains a degree of tamper-resistance and transaction finality (i.e. immutability).

These two attributes allow for a high degree of trust in the data on-chain. However, when personal data[2] is written on a blockchain (be it a permissionless or permissioned network), the decentralised and tamper-resistant attributes give rise to issues with **accountability** and **immutability** in complying with the obligations under the PDPA.

What Is Considered On-Chain Personal Data?

When personal data is published on, or accessible via, a blockchain in **cleartext**, it is considered to be "on-chain personal data". This may include:

a. Personal data that is captured as part of the on-chain transaction record (e.g. personal details such as name, address and contact number that constitute part of the metadata of an on-chain transaction).

b. Personal data that is stored off-chain but
   - Is stored in cleartext;
   - Is accessible via links that are stored on-chain; and
   - Is accessible to all participants in the blockchain without access control.

Such data is functionally equivalent to being hosted on-chain in cleartext.

[2] *Defined under the Personal Data Protection Act (2020) as "Data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access to."*

Accountability Issues

As data on blockchain is distributed across multiple nodes, there are challenges in determining and operationalising accountability over any distributed personal data:

A **Data Controllership.** To comply with 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 node operators:

a. In a **permissionless blockchain**, it is almost impossible to control access to on-chain personal data as any organisation (known or anonymous) can be a node operator and participate in the network.

b. In a **permissioned blockchain**, as the participants and node operators are generally curated and known by the blockchain operator, access to the chain can be controlled.

As a result, organisations may be better-positioned to control the access and use of personal data through technical controls (e.g. encryption or off-chain implementations with access control) or contractual controls (e.g. terms and conditions of use and access to participants) in a permissioned blockchain as opposed to a permissionless blockchain.

B **Transfer Limitation Obligation.** The Transfer Limitation Obligation ("**TLO**") requires personal data transferred overseas to be protected to a standard comparable with the Data Protection Provisions in the PDPA. If an organisation commits personal data on a blockchain with nodes spanning multiple jurisdictions, it will have to ensure that these jurisdictions have comparable protections to comply with the TLO.

C **Consent and Purpose Limitation.** Generally, the PDPA prohibits organisations 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 his or her personal data for a specific purpose. This presents a challenge in a permissionless blockchain, where data written on-chain is publicly accessible by all participants (e.g. node operators, ASPs and participating organisations), making it impossible for organisations to effectively establish control over the collection, use and disclosure of the data by another participant.

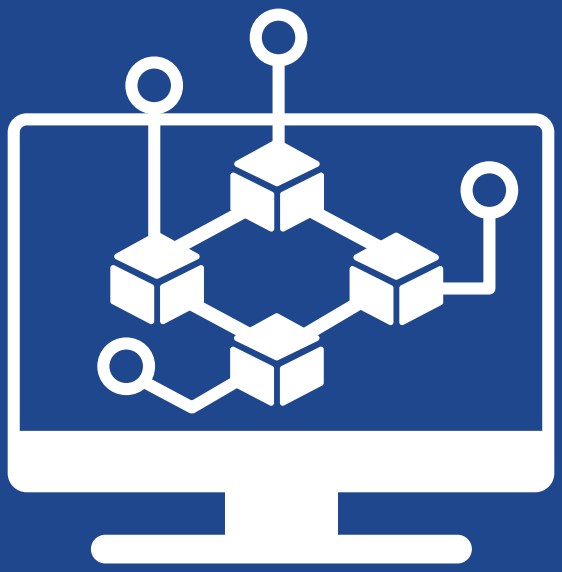
Immutability Issues

The immutable nature (i.e. tamper-resistance and finality) of data committed on the blockchain may give rise to the following challenges:

D **Protection Obligation.** Technical measures (e.g. encryption) to prevent the unauthorised disclosure of personal data can be part of reasonable arrangements by an organisation to protect personal data. However, in the case of encrypted personal data stored on a permissionless blockchain, the effectiveness of such protection mechanisms can be expected to degrade over time as threat actors' methods and computing power to break these mechanisms improve.

E **Retention Limitation Obligation.** Generally, if an organisation has fulfilled the purpose of collecting a piece of data, and there is no further business or legal requirement for data retention, the organisation should dispose the data. It can do so either by securely erasing it or stripping personal identifiers from the data. However, as the data committed on-chain is immutable, it cannot be erased or modified. Therefore, 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. via 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. As a result, this Guide will take a risk-based approach in recommending DPbD best practices for permissionless and permissioned types of networks in the following sections.



PART II: DESIGNING BLOCKCHAIN APPLICATIONS FOR PDPA COMPLIANCE

CONSIDERATIONS AND RECOMMENDATIONS FOR PERSONAL DATA ON PERMISSIONLESS BLOCKCHAIN NETWORKS

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 to the PDPA for organisations on a permissionless blockchain network.

Accountability Issues on Permissionless Networks

In a permissionless network, it is neither practical nor possible to implement or enforce any accountability obligations on entities in the network for the following reasons:

A. Any personal data that is committed on-chain is replicated on multiple nodes in the network. This makes the data publicly accessible to and usable by anyone (i.e. the public) who is participating in the permissionless network.

B. As no operator controls participation in a permissionless network, it is not possible to assert data controllership or enforce any protection obligations on participants for personal data written on-chain.

C. It is also not possible to control, or even 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.

Therefore, the PDPC would consider 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 for public disclosure has been obtained from the concerned individuals, or if the personal data is already available publicly.

Immutability Issues on Permissionless Networks

As discussed in Part I above, the immutable nature of blockchain networks means that data committed on-chain stays on it permanently as long as the blockchain network exists.

Such persistence of on-chain data also means that organisations cannot take for granted that any anonymised or encrypted data on permissionless blockchains, which is open and public in nature, will remain anonymised or encrypted in the long term. As long as there are operating nodes, threat actors will be able to access the publicly available data to:

A. Conduct **re-identification attacks** where anonymised datasets are analysed to discern the identity of the associated data subjects; or

B. **Decrypt encrypted data** uploaded on the blockchain via brute-force attacks or emerging methods such as quantum decryption.

Baseline Recommendation for Personal Data Protection on Permissionless Blockchains

In view of the above considerations, the PDPC recommends that as a baseline best practice for permissionless blockchains:

- 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.
- 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.

CONSIDERATIONS AND RECOMMENDATIONS FOR PERSONAL DATA ON PERMISSIONED BLOCKCHAIN NETWORK

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

Accountability Issues on Permissioned Networks

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. This means that all node operators are in possession of the data, thereby inadvertently increasing the regulatory burden on them.

Operators of permissioned blockchain networks should therefore ensure that personal data is well protected and is only accessible by or disclosed to authorised blockchain participants that have a business purpose for accessing the data. This will subject organisations to personal data protection obligations only with respect to the data that they are authorised to access. Some of the measures which blockchain operators can implement include:

A Curating participation in the network to only authorised organisations and imposing binding requirements on them via the consortium agreement. Such binding requirements could include restrictions on the kind of data that can be written on the network (further backed with technical controls) and restrictions on the behaviours of participants (e.g. prohibiting attempts to decrypt ciphertext).

B Admitting participation by organisations that can ensure adequate protection to personal data in all their nodes and data centres or sub-processors to which the data is transmitted to and stored on, so as to comply with the TLO. Such compliance can be ensured in the following ways:

- Admitting participants only from jurisdictions with comparable standards of protection;
- Ensuring binding contractual obligations for comparable protection through consortium agreements between the operator and participants[3]; or
- Requiring participants to obtain specified certification such as the Asia-Pacific Economic Cooperation ("**APEC**") Cross Border Privacy Rules ("**CBPR**") or Privacy Recognition for Processors ("**PRP**").[4]

C Requiring participants to encrypt or anonymise personal data on-chain using industry standard algorithms or practices, so that only authorised participants are able to access the data with the decryption keys or identity matching tables provided through off-chain channels.

D Monitoring and enforcing against any perpetrators of personal data breaches on the network.

Where appropriate, operators can leverage various consent exceptions under the PDPA, such as business improvement, deemed consent by contractual necessity or legitimate interests, as a legal basis to allow the participants to collect, use and share personal data under those circumstances without the need for consent from individuals.

The blockchain operator can also reduce the compliance burden on ASPs and node operators through contracts that define their processing of on-chain data as being on behalf of the operator, thus making the latter data intermediaries over that data.

[3] *Examples include the ASEAN Model Contractual Clauses (MCCs) for Cross Border Data Flows: template contractual terms and conditions that may be included in the binding legal agreements between businesses transferring personal data to each other across borders. Consortia may consider adapting these clauses in their contracts with participating organisations.*

[4] *Refer to this link for more details on the certifications.*

Immutability Issues on Permissioned Networks

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 than on permissionless blockchains. Besides protecting the data, protection mechanisms such as encryption also help overcome immutability issues.

Blockchain operators and participating organisations can comply with **correction** and **retention limitation** obligations by:

A Inserting new entries with encrypted corrected data; and

B Mandating secure disposal of the decryption keys of outdated data by other participants, rendering the data indecipherable.

It is also advisable to thoroughly document the process of identifying and deleting all copies of decryption keys, such that participants can stand up to independent scrutiny. Keeping records on the number of copies and location of the decryption keys is a good practice that can add credibility to this process.

Baseline Recommendation for Personal Data Protection on Permissioned Blockchains

In view of the above considerations, the PDPC recommends that as a baseline best practice for permissioned blockchains:

- 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.
- Blockchain operators should implement and effectively enforce legally binding consortium agreements or contracts to ensure PDPA compliance from participants (including ASPs, node operators and participating organisations) 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 (e.g. protection, correction and retention limitation obligations).

(continued on the next page)

Baseline Recommendation for Personal Data Protection on Permissioned Blockchains

(continued from the previous page)

- Blockchain operators should also regularly review these technical measures (e.g. encryption or other privacy preserving technologies) 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 (e.g. decryption and encryption keys); and
  - Technological developments are monitored and regularly reviewed to ensure the implemented protection measures stay relevant.

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 need not necessarily write personal data on-chain to still benefit from the decentralised and tamper-resistant nature of blockchain networks. They can instead consider **off-chain approaches that store personal data in centralised data repositories, while only writing representations of the personal data on-chain.**

An Off-Chain Approach to Blockchain Design

- 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 of the link to the off-chain database should be written on-chain. Hashes are cryptographically generated strings that serve as irreversible, 1-1 representations of the hashed data. Any change in the underlying data will generate a completely different hash. This allows the hash to be used as a digital signature that, if written on-chain, can serve as an immutable verification of the underlying data's integrity.

(continued on the next page)

An Off-Chain Approach to Blockchain Design

(continued from the previous page)

- 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.

In this approach, organisations are required to take a holistic view. They have to ensure that their off-chain storage solutions containing the personal data are also sufficiently protected[5] to prevent unauthorised access.

Under the above 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.

Such an off-chain approach can thus be used to fulfil personal data protection obligations in both permissionless and permissioned networks.

Other Approaches Under Development

In addition to 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. This approach can enable ASPs to design applications that enable personal data to be stored and exchanged entirely off the permissionless network. Such emerging approaches include:

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. An example of a hybrid blockchain approach is XinFin, which comprises a public state shared with all blockchain members, but gives them the ability to host private sub-networks that can be hidden from the rest of the network.[6]

[5] *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.*

[6] *Enterprise Ready Hybrid Blockchain (xinfin.org)*

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. Examples of such solutions include:

- **Nested blockchains** — secondary chains built upon the main chain.
- **State channels** — solutions that allow users to quickly transact with each other off-chain and publish the proof of their transaction on the main network.[7]
- **Zero-knowledge proofs** — solutions which enable sharing of proofs of personal data credentials between users without the need to share underlying personal data. Examples of these include the Baseline Protocol, an open-source initiative that aims to "enable confidential and complex collaboration between enterprises without leaving any sensitive data on-chain", and the Nightfall 3 set of tools from Ernst & Young.[8]

As blockchain use cases evolve, blockchain networks and foundations are becoming more aware of the challenges in complying with applicable data protection laws, and are developing solutions to enable prospective operators and participants to surmount such challenges.

[7] *Blockchain Technology: Layer-1 and Layer-2 Networks | Gemini*
[8] *Baseline | The Baseline Protocol an Oasis Open Project (baseline-protocol.org)*

ANNEX: DEVELOPING A DATA PROTECTION MANAGEMENT PROGRAMME FOR BLOCKCHAIN

If personal data is involved in the blockchain application, regardless of whether it is stored or processed on-chain or off-chain, the blockchain operator should develop and implement policies and practices that foster awareness and accountability over personal data in all blockchain participants.

In order to do this, the blockchain operator should consider implementing a ("**DPMP**"). As part of the DPMP, the blockchain operator should, where applicable:

A Establish an oversight committee for the blockchain consortium, where relevant.

B Ensure that the data protection officer ("**DPO**") 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. This includes defining what constitutes authorised access, who can obtain authorised access and what data can or cannot be committed on- and off-chain (e.g. only encrypted data can be committed on-chain). Where possible, use legally binding mechanisms (e.g. contractual consortium agreements and terms of use) and get all participants (including ASPs, node operators and participating organisations) to agree to abide by these policies as a pre-condition for joining the network.

D Conduct a Data Protection Impact Assessment ("**DPIA**") to identify and assess potential risks to personal data in the blockchain network and application. The DPIA should:

i. Identify the personal data accessed on and collected from the blockchain, as well as the reasons for such access and collection.

ii. Identify how the personal data flows through the network and processes.

iii. Identify the potential risks of personal data being captured and committed in-clear on the blockchain against the requisite processes in place to ensure PDPA compliance.

iv. Address the identified risks by implementing changes to the design of the network or application, or introducing policies.

v. Check if risks are adequately addressed before the blockchain network and application are implemented.

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.

Organisations interested to participate in blockchain network consortia should ensure that the blockchain operator has done its due diligence to implement the above best practices before joining a permissioned network.

Further details relating to the establishment of a DPMP and DPIA can be found in the *Guide on Developing a Data Protection Management Programme*[9] and *Guide on Data Protection Impact Assessment*.[10]

[9] *Refer to PDPC | Guide on Developing a Data Protection Management Programme*
[10] *Refer to PDPC | Guide on Data Protection Impact Assessments*

Exercising due diligence in adopting applications and services from third-parties or data intermediaries

Where a blockchain operator chooses to rely on third-party applications or data intermediaries to perform certain blockchain functions, it should take the following due diligence measures:

A. Understand and evaluate personal data management and cybersecurity capabilities of the third-parties or data intermediaries (e.g. their blockchain architectures and smart contracts design) to identify any associated risks before deploying their applications or services.

B. Ensure proper testing of third-party applications before deploying them onto the blockchain.

C. Establish the business objectives and requirements and data protection obligations of data intermediaries to whom processing of personal data is outsourced, and incorporate them into the outsourcing contracts.

D. Ensure that the data intermediary possesses the requisite capabilities to safeguard the personal data being processed. This includes determining if the data intermediary has established proper internal policies, processes and staff training for data protection, as well as compliance or certification under any relevant industry standards or security practices.

Further details related to the management of data intermediaries can be found in the *Guide on Managing Data Intermediaries under the PDPA*.[11]

[11] *Refer to PDPC | Guide on Managing Data Intermediaries*

ACKNOWLEDGEMENTS

The PDPC and Infocomm Media Development Authority (IMDA) express their sincere appreciation to the following organisations for their valuable feedback in the development of this publication (in alphabetical order):

- Attorney-General's Chambers of Singapore
- Blockchain Association of Singapore
- Baker McKenzie Wong & Leow
- Contour
- Ethereum Foundation
- Government Digital Services, GovTech
- Law Society of Singapore's Cybersecurity and Data Protection Committee 2021/2022
- Norton Rose Fulbright Asia LLP
- Singapore Fintech Association
- Temasek

The following sources were referenced in this Guide.

- Commission Nationale Informatique et Libertés. *Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*, September 2018, https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf
- Panel for the Future of Science and Technology. *Blockchain and the General Data Protection Regulation – Can Distributed Ledgers by Squared with European Data Protection Law?* by Finck, Michelé, 2018, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf
- International Organisation for Standardisation. *Terminology of Blockchain and Distributed Ledger Technologies (ISO/DIS Standard no. 22739:2020)*, July 2020, https://www.iso.org/standard/73771.html
- NIST. *NISTIR 8202: Blockchain Technology Overview*, by Yaga, Dylan; Mell, Peter; Roby, Nik; Scarfone, Karen, October 2018, https://csrc.nist.gov/publications/detail/nistir/8202/final
- Cryptopedia Staff. *Layer-1 and Layer-2 Blockchain Scaling Solutions,* March 9, 2022, https://www.gemini.com/cryptopedia/blockchain-layer-2-network-layer-1-network, accessed in November 2021.
- Baseline Protocol. *What is the Baseline Protocol?* https://www.baseline-protocol.org/about, accessed in November 2021.
- XinFin. *About Us*, https://xinfin.org/about, accessed in November 2021.

#SGDIGITAL

Singapore Digital (SG:D) gives Singapore's digitalisation efforts a face, identifying our digital programmes and initiatives with one set of visuals, and speaking to our local and international audiences in the same language.

The SG:D logo is made up of rounded fonts that evolve from the expressive dot that is red. SG stands for Singapore and :D refers to our digital economy. The :D smiley face icon also signifies the optimism of Singaporeans moving into a digital economy. As we progress into the digital economy, it's all about the people — empathy and assurance will be at the heart of all that we do.

BROUGHT TO YOU BY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE