Report on Data Privacy Regulations

Applicable to Blockchain Technology in Various Jurisdictions Worldwide

2021–2022 Edition

By the Privacy Working Group of INATBA

International Association for Trusted Blockchain Applications

MAY 2022

Table of Contents

Executive Summary

Around the globe, different privacy-related regulations apply, but how do these various regulations impact blockchain technology? Which jurisdictions are the most favourable for technology applications and which are the most limiting? Through the involvement of leading international privacy experts, the Privacy Working Group of the International Association for Trusted Blockchain Applications (INATBA) has sourced valuable information on how regulations from different jurisdictions affect the use of blockchain technology with regard to data protection and privacy.

As the created chains are operated and maintained in a decentralised network, the nodes forming that network may be located in different jurisdictions and can thus be subject to various data protection regulations. This decentralised situation results in a significant burden of verifying compliance of the blockchain-based solution as there is not only one particular data protection regulation to abide by, but potentially many other ones to follow. This is especially relevant for large public permissionless blockchains, where there is virtually no control over nodes joining the network from different countries.

Generally, jurisdictions with comparatively high legal certainty are considered more attractive for innovative technology such as blockchain. In 12 out of the 17 regions (including the European Economic Area as a whole) assessed, there was some reasonable level of legal certainty. Across the remaining five regions, legal certainty was limited when this report was written. Yet, a defined legal framework can be as much an asset in terms of ensuring legal certainty as it can lead to major challenges in terms of compliance. While regulations may provide legal clarity, they may also be highly restrictive. For example, Russia requires data to be stored domestically, which is not conducive to decentralised environments that span multiple countries.

At the time of writing, multiple jurisdictions have recently implemented changes or are planning to implement changes regarding data protection legislation or other adjacent regulations. For example, the European Union's Digital Finance Package[1], which includes the proposed regulation on Markets in Crypto-Assets (MiCA)[2], might have an effect on data protection aspects of asset-related blockchain technology.

Please be advised that the information contained in this report is current as of the date of publication of this report.

[1] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593.

Introduction

Blockchains are shared, synchronised peer-to-peer digital databases that are maintained by an algorithm and stored on multiple nodes. They form decentralised networks. Eventually, blockchains become ledgers, which may store different types of data, including personal data. When that is the case, various data protection regulations may become applicable to the blockchain technology, raising certain rights and obligations for different actors of the blockchain networks.

The structure and nature of blockchains may potentially lead to numerous problems regarding data protection compliance, such as:

I. allocation of responsibility for compliance,

II. principles of data minimisation and purpose limitation,

III. exercising of data subjects rights,

IV. blockchains' immutability,

V. anonymisation techniques or

VI. cross-border data transfers.

As the created chains of blocks are operated and maintained in a decentralised network, the nodes forming that network may be located in different jurisdictions and thus be subject to multiple data protection regulations. This generates a significant compliance audit burden on blockchain-based solutions, as there is not just one particular data protection regulation to comply with, but potentially several. This is particularly relevant for large, public, permissionless blockchains, where there is close to no control over which nodes join the network over different jurisdictions.

Since it was implemented in May 2018, the EU's General Data Protection Regulation **(GDPR)** generated significant commentary concerning its applicability to blockchain technology. For instance:

- The French DPA – CNIL (*Commission nationale de l'informatique et des libertés*), officially addressed the applicability of the GDPR to blockchain technology and its potential use-cases in a specific set of guidelines; [3]

- The EU Blockchain Observatory and Forum – an initiative sponsored by the European Commission that provides analyses and discussion forums concerning blockchain technology – released a thematic report "Blockchain and the GDPR"; [4]

- A study "Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?" was written at the request of the Panel for the Future of Science and Technology

[3] https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.
[4] https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

(STOA) of the Secretariat of the European Parliament.[5]

Numerous scholars and experts have similarly issued a number of other reports in this field.

Surprisingly, however, there is limited written guidance about compliance with data protection regulations in other jurisdictions in terms of personal data stored on blockchains. The lack of a comprehensive overview of existing data protection regulations and their applicability to blockchain technology poses a significant challenge for further development of this cutting-edge technology.

This report aims to address these concerns and provide the industry with an overview of data protection regulations in jurisdictions considered particularly important for the development of blockchain technology. In this report, the following countries were selected based on their relevance in the blockchain industry and crypto market:

- The European Union,
- Australia,
- Brazil,
- Canada,
- China,
- Hong Kong,
- India,
- Israel,
- Japan,
- Russia,
- Singapore,
- South Africa,
- South Korea,
- Switzerland,
- Ukraine,
- the United Kingdom, and
- the United States of America.

To help blockchain companies and data protection practitioners to navigate these blurry legal waters, the INATBA Privacy Working Group prepared the following set of questions to be answered based upon the laws of the jurisdictions included in

[5] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

the aforementioned list:

1. What are the legal acts regulating data privacy in your jurisdiction?
2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?
3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.
4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.
5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?
6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?
7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?
8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?
9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?
10. Is it necessary to notify processing activities to any authorities?
11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?
12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?
13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?
14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?
15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?
16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of

transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

While some of the questions are more universal and refer to general characteristics of the data protection regime, others explicitly address privacy compliance issues specifically concerning blockchain technology.

The core part of this report opens with a chapter concerning the GDPR. It is then followed by country-specific chapters organised in an alphabetical order. These chapters were prepared by renowned experts in the field of data protection that kindly agreed to cooperate with the Privacy Working Group on this project.

* *

*

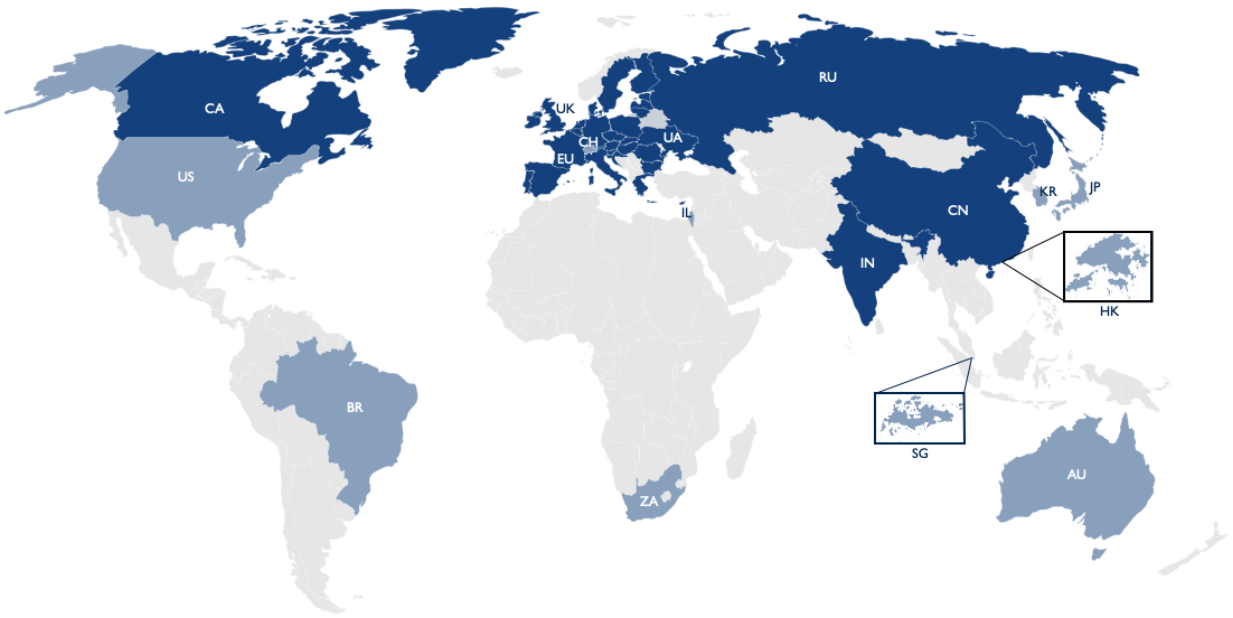
Since its launch in April 2019, INATBA (inatba.org) has established itself as the pre-eminent convener in the global blockchain ecosystem, offering developers and users of distributed ledger technology (DLT) a forum to interact with regulators and policy-makers with the overarching mission of bringing blockchain technology to the next stage.

The Privacy Working Group of INATBA gathers privacy and blockchain experts from various jurisdictions. The Working Group's goals are as follows:

1. analyse the applicability of privacy regulations to blockchain technology,
2. advocate for blockchain-friendly interpretation of privacy regulations, and
3. educate the industry about privacy regulations applicable to blockchain technology.

Cross-Country Comparison

Below is a map of the countries reviewed in this document. Light blue represents little or light regulation while dark blue represents more complex or comprehensive regulation. Blank countries have not been surveyed.



The table below presents a summary of the responses categorised by general question theme. The data in the table is based on the inputs from the contributors and required some assessment; nevertheless, the results provide a solid overview of the complexity of privacy regulations across the jurisdictions surveyed.

Overview of general data protection legislation and applicability to blockchain ledgers in various jurisdictions

	EU	AU	BR	CA	CN	HK	IN	IL	JP	RU	SG	SA	KR	CH	UA	UK	US
Jurisdictional completeness and precedent																	
3. Have authorities specifically addressed blockchain/DLT?	1	0	0	1	1	0	1	1	0	0	0	0	0	0	0	1	1
4. Do data protection rules address specific actors?	2	1	2	2	2	2	2	0	2	1	2	2	2	2	2	2	1
5a. Do data protection rules define personal data?	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
5b. Does it categorise personal data?	2	2	2	2	1	1	2	1	2	2	0	2	2	2	2	2	2
6. Do data protection rules define pseudonymisation and/or anonymisation?	1	1	2	2	1	0	1	/	1	2	0	1	1	0	2	2	2
7a. Is there specific legislation/regulation on blockchain?	0	0	0	1	1	0	1	1	1	2	1	0	1	1	0	0	1
7b. If so, does it refer to data privacy?	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0
8a. Has anonymisation techniques been addressed in the jurisdiction?	0	1	0	1	0	2	0	/	1	2	1	0	1	0	0	2	1
8b. Is such precedent relevant for blockchain?	0	1	0	1	0	0	0	/	1	2	1	0	1	0	0	1	1
Localisation and notification																	
9a. Must personal data be stored locally?	0	0	0	1	1	0	1	0	0	2	0	1	0	1	0	0	0
9b. Is international transfer addressed and allowed?	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2
10. Must authorities be notified of data processing activity?	0	1	0	1	1	0	0	2	0	2	0	1	0	1	2	2	0
Overview of defined rights in data protection rules																	
11a. Right to access & corrections?	2	1	2	2	2	2	2	/	2	2	2	2	2	2	2	2	1
11b. Right to be forgotten? Or some deletion?	2	0	2	1	2	1	2	/	1	1	0	1	2	1	1	2	0
11c. Right to restrict processing?	2	0	2	1	2	1	2	/	2	2	0	1	2	2	2	2	1
11d. Obligation of notifications?	2	0	1	1	1	1	1	/	1	1	1	2	2	2	2	2	1
11e. Right to portability?	2	0	2	2	2	0	2	/	0	0	0	0	1	0	0	2	0
11f. Right to object?	2	0	2	0	2	2	2	/	2	2	1	2	2	2	2	2	1
11g. Right to not be subjected to automated decisions?	2	0	2	0	1	1	1	/	1	2	0	2	0	0	2	2	0
Potential applicability of existing rules to blockchains																	
12. Would actors in a public blockchain be responsible?	1	1	1	0	2	1	2	/	1	1	0	1	1	1	1	2	1
13. Does data protection apply to private/permissioned blockchains?	2	1	2	2	2	1	2	0	1	2	2	1	1	1	2	2	1
15. Are there best practices for processing personal data on blockchains?	2	1	1	2	2	1	2	0	0	/	1	0	0	1	2	1	0
16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation?	0	0	1	2	0	1	0	2	1	/	1	1	2	2	2	1	2
Average value	1.26	0.65	1.22	1.26	1.35	0.91	1.35	0.39	1.09	1.43	0.67	1.04	1.13	1.09	1.3	1.57	0.91

Legend	
No answer	/
No / Not addressed or covered / No or unclear precedent	0
Partially / In some cases / Some precedent	1
Yes	2

Authors

INATBA PRIVACY WG – Contributors and Reviewers[6]

Giacomo Fedele, DNV

Colombe de Franqueville, Archipels

Paola Heudebert, Archipels (Privacy Working Group Co-Chair)

Ella Schröder, Lisk Foundation

Maitén Vilches, IOTA Foundation

EUROPEAN UNION

Giacomo Fedele, DNV

Paola Heudebert, Archipels (Privacy Working Group Co-Chair)

Silvan Jongerius, TechGDPR

Ella Schröder, Lisk Foundation

Maitén Vilches, IOTA Foundation

Marcin Zarakowski, Bitcoin Association

AUSTRALIA

Christine Bulos, RMIT Blockchain Innovation Hub

Aaron M. Lane, RMIT Blockchain Innovation Hub

BRAZIL

Tatiana Campello, Demarest Advogados

Betina Portella Cunha Ferreira, Demarest Advogados

Julia Davet Pazos, DSMA Azulay

CANADA

Luca Lucarini, Dentons

Chloe Snider, Dentons

Noah Walters, Dentons

[6] Please note that professional affiliation may have changed since the author's contribution to the report.

CHINA

Hu Ke, Jingtian & Gongcheng

Yuan Lizhi, Jingtian & Gongcheng

HONG KONG

Gabriela Kennedy, Mayer Brown

Karen H. F. Lee, Mayer Brown

Cheng Hau Yeo, Mayer Brown

INDIA

Anirudh Rastogi, Ikigai law

Sreenidhi Srinivasan, Ikigai law

Mayank Takawane, Ikigai law

ISRAEL

Smadar Peleg, Efficient Frontier

JAPAN

Ken Kawai, Anderson Mori & Tomotsune

Takeshi Nagase, Anderson Mori & Tomotsune

Huan Lee (Henry) Tan, Anderson Mori & Tomotsune

Kai Ishikawa, Anderson Mori & Tomotsune

RUSSIA

Maxim Lagutin, B-152

Maxim Zinovyev, B-152

SINGAPORE

Branson Lee, Blockchain Association Singapore

Dharma Sadasivan, BR Law Corporation

SOUTH AFRICA

Caitlin Gottschalk, Gottschalk Attorneys

Njabulo Kubheka, Gottschalk Attorneys

Kerry Bundy-Palmer, Gottschalk Attorneys

Patience Katiyo, Gottschalk Attorneys

SOUTH KOREA

Kijun Kwon, Kwon, Park & Rhee

Jungyoon Oh, Kwon, Park & Rhee

Kwanhoo Oh, Kwon, Park & Rhee

SWITZERLAND

Carmen De la Cruz Böhringer, LEXcellence AG

Ella Schröder, Lisk Foundation

UKRAINE

Vlad Nekrutenko, Legal Nodes

UNITED KINGDOM

Sam Mottahedan, Blockchain for Human Rights

Laura Scaife, Datultacy

UNITED STATES OF AMERICA

Odia Kagan, Fox Rothschild

Caroline A. Morgan, Culhane Meadows

EU General Data Protection Regulation

Authors
Giacomo Fedele, DNV
Paola Heudebert, Archipels (Privacy Working Group Co-Chair)
Silvan Jongerius, TechGDPR
Ella Schröder, Lisk Foundation
Maitén Vilches, IOTA Foundation
Marcin Zarakowski, Bitcoin Association

1. What are the legal acts regulating data privacy in your jurisdiction?

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 "General Data Protection Regulation" **(GDPR)**[7] is the most important data privacy legal act in the European Union. It sets the general framework for the protection of personal data in the EU. The regulation entered into force on 24 May 2016 and was applicable from 25 May 2018 onwards.

Despite the GDPR being a directly applicable regulation, it still leaves a margin of discretion for EU Member States to implement different specifications or restrictions on certain components of the set rules. In summation, the GDPR allows for about 50–60 possible national derogations. Therefore, when analysing particular processing activity, it may be also necessary to consider the applicable domestic data protection laws in individual EU Member States.

Because the GDPR also applies to the processing of personal data when targeting EU data subjects by non-EU entities and due to the so-called Brussels effect,[8] the GDPR essentially sets the "gold standard" for the protection of personal data for businesses operating on a global scale.

Other acts applicable to processing of personal data in the EU, that are significantly less important in the context of blockchain technology, are:

- Directive (EU) 2016/680 – the Data Protection Law Enforcement Directive: protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes (EU Member States were obliged to transpose it into their national laws by 6 May 2018);
- Regulation 2018/1725 – sets forth the rules applicable to the processing of

[7] Full name: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[8] The Brussels effect is the process of regulatory globalisation caused by the European Union de facto externalising its laws outside its borders through market mechanisms. Due to the Brussels effect, corporations end up being forced to comply with EU laws even outside of the EU's territory.

personal data by European Union institutions, bodies, offices and agencies as well as establishes the office of the European Data Protection Supervisor **(EDPS)**.

Finally, it is necessary to note that article 8 of the EU Charter of Fundamental Rights stipulates that EU citizens have the right to protection of their personal data.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

Each EU Member State has a national Data Protection Authority **(DPA)**, an independent public authority that uses investigative and corrective powers to supervise the application of the data protection law. Among other tasks, DPAs provide expert advice and handle complaints against the GDPR as well as domestic data protection regulations. Additionally, the EDPS's role is to ensure that EU institutions and bodies respect people's right to privacy when processing personal data.

Furthermore, the European Data Protection Board **(EDPB)**, an EU body composed of the heads of each DPA and the EDPS or their representatives, is responsible for ensuring the uniform application of the GDPR. The European Commission participates in the meetings of the EDPB without voting rights. The EDPS provides the secretariat for the EDPB.

The EDPB helps to ensure that the data protection laws are applied consistently across the EU and works to ensure effective cooperation amongst all DPAs. The Board issues various guidelines on the interpretation of core concepts of the GDPR but is also tasked with ruling on and issuing binding decisions on cross-border processing disputes. These duties allow the EDPB to ensure a uniform application of EU rules to avoid a single case potentially being dealt with differently across various jurisdictions. Before the GDPR was implemented, Article 29 Working Party **(Art. 29 WP)**, which acted as the independent European working party, dealt with issues related to the protection of privacy and personal data at the EU level[9]. Some of the guidelines issued by Art. 29 WP remain valid today.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

Currently, only the French DPA – CNIL (*Commission nationale de l'informatique et des libertés*), officially addressed the applicability of the GDPR to blockchain technology and its potential use cases in a specific guidance document.[10] The document incorporates rules on how to determine data controllers and data processors in blockchain architectures, roles and duties of these actors, advice on how to minimise risks for data subjects when processing is carried out on a blockchain and methods of ensuring effective exercise of data subjects' rights.

[9] Art. 29 WP's full name was "The Working Party on the Protection of Individuals with regard to the Processing of Personal Data" and it was established in 1996 by virtue of Article 29 of Directive 95/46/EC.
[10] CNIL — Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 6 November 2018, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context- personal-data.

It is worth mentioning that the Spanish DPA – AEDA (*Agencia Española de Protección de Datos*), in its joint paper with EDPS, addressed in detail the issue of using hash techniques by data controllers in their data processing activities, which is an essential factor in GDPR-compliance of blockchain technology.[11]

Finally, in its work programme for 2019/2020, the EDPB mentioned blockchain as one of the possible topics for further assessment and possible issuance of thematic guidelines[12].

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

The GDPR defines the following actors:

- "Data controller" refers to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- "Data subject" refers to an identified or identifiable natural person to whom "personal data" relates;
- "Processor" refers to a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Where two or more controllers jointly determine the purposes and means of processing, they shall be considered "joint controllers".

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

The GDPR defines Personal Data as "any information relating to an identified or identifiable natural person". This is a wide definition and should be interpreted broadly as any information that can (help to) directly or indirectly identify a specific individual.

Sensitive data ("special categories of personal data", defined in article 9) includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health and data concerning a natural person's sex life or sexual orientation. Such data may only be processed in exceptional circumstances (for example, after explicit consent from the data subject or in the vital interests of the data subject).

Personal data related to criminal offences or convictions requires additional

[11] AEPD, EDPS — Introduction to the hash function as a personal data pseudonymization technique, 30 October 2019, https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf.
[12] https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf.

protection and may only be collected as an exception, mainly when under the control of an official authority[13].

Additionally, the more sensitive the personal data is, the stronger the protection measures need to be under the accountability principle of the GDPR.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

In its article 4 (5), the GDPR defines pseudonymisation as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

In line with this interpretation, recital 26 specifies that pseudonymised data should still be considered information pertaining to an identifiable natural person. This is based on the fact that data subjects can be easily identified if the additional information is linked again to the pseudonymised personal data. Therefore, this data still falls within the scope of GDPR, unlike anonymous personal data. At the same time, pseudonymisation is considered as a technique that helps data controllers and processors to meet their data-protection obligations.[14] It is considered as an appropriate safeguard in articles 6, 25, 32 and 89.

Anonymisation is not defined in any EU Data protection rules. However, recital 26 of the GDPR provides sufficient information on the matter. Anonymous data is defined as "information which does not relate to an identified or identifiable natural person". Therefore, the outcome of anonymisation applied to personal data is that it is no longer possible to identify data subjects using all the means "reasonably" and "likely" to be used. Anonymisation can be seen as an erasure of such personal data given the current state of technology.

Art. 29 WP presented an opinion on anonymisation techniques.[15] The opinion provides further guidance on anonymisation techniques and supports the significantly high bar for what constitutes anonymous data. Important in the context of blockchain technology, the Art. 29 WP considered encryption and mere hashing as not sufficient to render the data anonymous. Interestingly enough, said opinion of the Art. 29 WP was not endorsed by the EDPB.[16]

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

There are no pieces of legislation at the EU level which specifically address using blockchain technology. Nevertheless, various EU legal acts may apply to a particular use case of DLT and blockchain.

---

[13] General Data Protection Regulation, op. cit., article 10. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32016R0679.

[14] Ibid., recital 28.

[15] Art. 29 WP — Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, https://ec.europa.eu/justice/article-29/ documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[16] EDPB — Endorsement 1/2018, https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents.pdf.

For instance, depending on the nature of a blockchain-based token, there are three recognised general categories of tokens: payment tokens, utility tokens and security tokens (there are also hybrid tokens which have features of more than one token category). Should the token meet the criteria of a financial instrument under the EU law, it would be considered as a security token and therefore fall under various legal acts forming the EU capital markets law (e.g., MiFID II[17], the Market Abuse Regulation[18], the Prospectus Regulation[19], the Transparency Directive[20], the Short-Selling Regulation[21]). Some payment tokens may also fall under the definition of e-money and would therefore be covered by the EU E-Money Directive[22] and possibly under the PSD 2.[23]

Moreover, the 4th and 5th Anti-Money Laundering Directives[24] impose obligations on EU Member States to have their AML laws at least covering service providers offering fiat-virtual currencies exchanges and custody of virtual currencies.

Furthermore, since various contracts concerning tokens are signed with consumers online, the EU consumer law will also apply, namely: the Consumer Rights Directive[25], the E-Commerce Directive[26] and the Directive on the distance marketing of consumer financial services[27].

Finally, because blockchains are ledgers that resemble databases, they would fall under the GDPR if they store and process any personal data in the European Economic Area **(EEA)** or data from EEA-based subjects when processing is associated with offering goods or services or monitoring their behaviour.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

Anonymisation and pseudonymisation techniques continue to be one of the most topical issues discussed in the context of blockchain/DLT compliance with the GDPR. To date, the EU has not taken an official position in assessing which techniques would definitively qualify as anonymising data (e.g., hashes) and

[17] Directive 2014/65/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0065&qid=1605789164153.
[18] Regulation (EU) No. 596/2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0596&qid=16057 89304253.
[19] Regulation (EU) 2017/1129, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1129&qid=160578936 9505.
[20] Directive 2013/34/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0034&qid=1605789435888.
[21] Regulation (EU) No. 236/2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R0236&qid=1605789 499123.
[22] Directive 2009/110/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0110&qid=1605789567249.
[23] Directive (EU) 2015/2366, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366&qid=1605789614736.
[24] Directive (EU) 2015/849, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849&qid=1605789669731; Directive (EU) 2018/843, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843&qid=1605789747589.
[25] Directive 2011/83/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0083&qid=1605789799455.
[26] Directive 2000/31/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000L0031&qid=1605789847394.
[27] Directive 2002/65/EC, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0065.

therefore exclude this from the scope of the GDPR. Notably, Art. 29 WP has stated in its opinion document that pseudonymisation is not a method of anonymisation as "it merely reduces the linkability of a dataset with the original identity of a data subject, and is accordingly a useful security measure".[28]

At the same time, GDPR refers to the risk-based approach and formulates a test that should be employed to determine whether or not data is considered personal, namely whether the controller or another person are able to identify the data subject by using "means reasonably likely to be used"[29]. In line with this, the Spanish Data Protection Authority has assessed that hashing may be viewed as an anonymisation technique after conducting a thorough risk assessment that also must include evaluation of organisational measures guaranteeing the removal of any information that allows for re-identification as well as the reasonable guarantee of system robustness beyond the expected useful life of personal data.[30]

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

The GDPR does not require data controllers and data processors to store personal data locally within the EEA; international data transfers are possible. However, whenever personal data is transferred outside of the EEA, an adequate level of protection must be guaranteed. This can be done in compliance with the GDPR in one of the following ways:

A. Personal data is transferred to a country for which the European Commission has issued an adequacy decision.

B. There are appropriate safeguards implemented:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules;
- model clauses (i.e., standard contractual clauses);
- an approved code of conduct together with binding and enforceable commitments;
- an approved certification mechanism together with binding and enforceable commitments.

10. Is it necessary to notify processing activities to any authorities?

No, the GDPR does not require data controllers or data processors to notify data protection authorities of processing activities. Nevertheless, the GDPR imposes certain obligations on data controllers and processors whenever a breach of personal data occurs.

[28] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, p. 3.
[29] GDPR, recital 26. See also EPRS — Blockchain and the General Data Protection Regulation, July 2019: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, p. 31.
[30] https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf, p. 23.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

The GDPR develops the user rights in Chapter III, articles 12–23. They can be categorised in three main areas: obligations of data controllers, rights to be exercised by subjects and restrictions that apply to subject rights requests.

The obligations of data controllers regarding the grounds for subjects to exercise the rest of its rights include: transparency of data collected by the data controller, regardless of whether it has been obtained directly or indirectly from the subject as mentioned in articles 12, 13 and 14, and the right to access personal data by the data subject as mentioned in article 15.

In other words, a subject has the right to check whether a data controller has any subject personal information and what is the purpose of holding such data by sending a data access request to the data controller. This is relevant because personal data collected has to have a purpose, which is known to the data subject in advance, and any change regarding this purpose has to be communicated to and permissioned by the subject.

The right to be forgotten does exist and is provided for in article 17. However, the tension between blockchain technology and the right of erasure is present; partially due to the technology itself and partially to the imprecise meaning of the term “erasure”.

A subject can then exercise the following rights:

- Article 16: Right of rectification for incorrect or incomplete data;
- Article 17: Right of erasure or “right to be forgotten”;
- Article 18: Right to restriction of processing;
- Article 19: For these rights, the data controller has the obligation to notify to whom the subject personal data has been shared or sent, with respect to new limits or actions;
- Article 20: Right to data portability;
- Article 21: Right to object;
- Article 22: Right to not be subjected only by automated decision-making, including profiling;
- Article 23: Restrictions or exercising of subject rights that can be legislated by a Member State in order to safeguard the national security, defence, public security, etc.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

Public blockchain networks allow anyone to access and decide how they participate on the blockchain. Actors considered to have a controller and/or (sub-)processor role in the data processing procedure of personal data could thus be regulated/responsible under the data protection legislation. Although there is a fairly clear legal framework for the assessment of determining controllership and processors under the GDPR (including the following case law and guidance), current legal discourse expresses uncertainty as to whether this jurisprudence is adequate as it was developed without the contextual understanding of decentralised networks. To further this point, the main contentions that have been made include:

- the notion of data subjects, controllers and processors (dual-role dilemma);
- the applicable principles for Data Processing;
- the applicable Data Subject Rights;
- territoriality.

Despite blockchain being one of the possible topics that the EDPB aimed to explore and the European Data Protection supervisor recently mentioned the importance of discussing blockchain, there has been no specific guidance under the GDPR as to which actors will be regulated/responsible and what this would look like.[31]

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The GDPR applies to all processing of personal data. This means that whenever personal data is on a blockchain, the GDPR applies. Depending on the particular setup, there are different means of application. On private blockchains, the participants are typically known and therefore the required data processing agreements can be concluded with relative ease. On public blockchains, the GDPR-defined roles of controller, processor and joint-controller are not as easily determined, and it is generally more challenging to obtain a binding agreement in place between typically unknown actors.

While both private and public blockchains face the theoretical challenge of information being indiscriminately distributed to all participants within the network, a public blockchain network encounters an additional challenge as it "publishes" information as it becomes available to anyone accessing the chain. It is up to Member States to establish derogations on publishing information, resulting in requirements that differ by country.

[31] European Data Protection Board, "EDPB Work Program 2019/2020", https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf, p. 3.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

Naturally one of the main issues concerns the data subject's right to be forgotten. However, the definition of "erasure" in the GDPR article 17 is unclear, which makes it even more difficult to determine whether a blockchain is able to comply with the said article. There are some indications in the case law which do suggest that erasure would not necessarily mean a complete destruction of data, but rather an erasure from search results could be enough.[32] Also other means such as anonymisation and "putting beyond use" have been discussed as definitions of the meaning of erasure in article 17.

As mentioned above, one further challenge is that it's highly unclear who or which party should be considered the data controller. It has been argued that the following parties could fulfil the definition of a controller: software developers, miners, nodes and users.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

Whether on or outside the blockchain, when it comes to data protection, the best practices in regard to data privacy are always to follow the principles of data minimisation, storage and purpose limitation and, maybe most importantly, privacy by design.

To that extent, a good practice for processing personal data on both public and private blockchain consists of the use of so-called Zero Knowledge Proof (ZKP) protocol such as zk-SNARK. The ZKP protocols appear to be among the most protective in the world for the protection of the privacy of users of online services. They guarantee a significant limitation on use of personal identity attributes by going well beyond the principle of data minimisation, which is difficult to respect in practice. It should be noted that the European Parliament has already recognised the potential of the ZKP to resolve the conflict between data minimisation and multi-party data verifiability. The European Parliament had called for funding of research in this area by recognising the strong potential of blockchain technology.[33]

The application of the layer 2 approach can also be beneficial. Layer 2 protocols create a secondary framework, where blockchain transactions and processes can take place independently of the layer 1 (main chain). For this reason, these techniques may also be referred to as "off-chain" scaling solutions. Layer 2 solutions are suitable for implementing GDPR's compliance processes notably allowing for data subjects rights implementation. In that paradigm, it is good practice to use the main blockchain networks to store immutable proof that certain data exists, rather than to store the data itself.

[32] Case C-131/12 Google Spain.
[33] https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html.

In the absence of an official recommendation, it is always recommended to apply a common sense of fairness and proportionality as well as "good faith" effort to take in consideration general GDPR principle.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

The latest changes introduced in June 2019 in the FATF standards on new technologies, aiming at regulating so called virtual assets and virtual asset service providers, have provided new and similar obligations for virtual asset service providers, with the purpose to facilitate the traceability of transfers of virtual assets. Thus, under those new requirements, virtual asset transfer service providers must accompany transfers of virtual assets with information on their originators and beneficiaries, that they must obtain, hold, share with counterpart at the other hand of the virtual assets transfer and make available on request to appropriate authorities.[34]

Currently, no aspects of the FATF's "travel-rule" have been implemented into the European AML legislation. However, at the member-state level, some countries have started the alignment with the FATF's "travel-rule" requirements. The legislative works are in progress at the time of writing. Personal data that will most likely need to be shared include name of the payer/payee, account numbers, the payer's address, country, official personal document number, customer identification number or date and place of birth.

While it is not possible at the time of writing to anticipate precisely what the European transposition of the Travel Rule will consist of, certain remarks should be made at this stage:

- The type of the data envisioned (name, surname, address, wallet address, public key and potentially previous transactional history stored on blockchain) is core identity data especially when processed in combination with each other, potentially resulting in identity theft if breached. Hence, it is crucial that the processing is done in a secure manner.

- The exceptionally broad definition of a VASP[35] may lead to treating as VASPs actors which have none or very little control, especially in the context of decentralised finance (DeFi) projects. A question arises whether they should be considered data controllers in regard to the personal data processed for the purpose of compliance with the Travel Rule. The same question arises

[34] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0422&from=EN.

[35] Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. *Source:* https://www.fatf-gafi.org/glossary/u-z/.

from the current text of the proposal to amend the 2015 Regulation on Transfers of Funds.

- Given the borderless nature of virtual assets transfers, personal data may be shared with VASPs which are neither based in the European Economic Area nor a jurisdiction providing an adequate level of protection. The GDPR provides for a general prohibition of such cross-border data transfers unless other appropriate safeguards are undertaken. One such safeguard is the Standard Contractual Clauses (SCCs) adopted by the EU Commission, which would require VASPs to agree to be contractually bound to specific obligations, even though these foreign VASPs may not be legally required to do so in their relevant domestic laws. Nevertheless, in the aftermath of the European Court of Justice's decision in the *Schrems II* case in 2020, the mere incorporation of SCCs may not provide sufficient basis for the transferring of data to third countries.

Country-Specific Chapters

Australia

Authors
Christine Bulos, RMIT Blockchain Innovation Hub
Aaron M. Lane, RMIT Blockchain Innovation Hub

1. What are the legal acts regulating data privacy in your jurisdiction?

There are various pieces of legislation in place to regulate data privacy and protection in Australia, through a mix of federal, state and territory laws.

On a national level, Australian data is principally governed by the *Privacy Act 1988* (Privacy Act) along with the *Privacy Regulations* 2013. The Privacy Act was introduced in 1988 and commenced in 1989. Originally designed to regulate how Australian Government agencies manage personal information, the Act was subsequently expanded to cover consumer credit reports by consumer credit reporting bodies and credit providers (1991), and private sector organisations with an annual turnover of more than $3 million – although some exceptions apply (2001). Significant changes to the legislation were made in 2014 and a notifiable data breach scheme was introduced in 2018. Amendments providing for a new privacy code for online platforms are currently before the Australian Parliament.

Most states and territories in Australia have additional legislation, including:

- *Information Privacy Act 2014* (Australian Capital Territory);
- *Information Act 2002* (Northern Territory);
- *Privacy and Personal Information Protection Act 1998* (New South Wales);
- *Information Privacy Act 2009* (Queensland);
- *Personal Information Protection Act 2004* (Tasmania); and
- *Privacy and Data Protection Act 2014* (Victoria).

Additionally, there are other parts of state, territory and federal legislation that relate to data protection. For example, the following all impact privacy and data protection for specific types of data or activities:

- *Telecommunications Act 1997* (Cth);
- *Criminal Code Act 1995* (Cth);
- *National Health Act 1953* (Cth);
- *Health Records and Information Privacy Act 2002* (NSW);

- *Health Records Act 2001* (Vic); and
- *Workplace Surveillance Act 2005* (NSW).

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

The Office of the Australian Information Commission (OAIC) is the independent national regulator for privacy and freedom of information at the federal level. The OAIC has broad powers including the authority to receive complaints, conduct investigations, make determinations, accept enforceable undertakings, and apply to the court to seek civil penalties.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

The OAIC has not issued any public guidance or determinations. However, in 2019, the OAIC (along with privacy officials in Albania, Burkina Faso, Canada, the European Union, the United Kingdom, and the United States) voiced concerns about "the privacy risks posed by the Libra digital currency and infrastructure".[36]

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

The Privacy Act incorporates the Australian Privacy Principles (APP) which are legally binding and set out obligations for an "APP Entity" in dealing with data – whether that be the collection, usage, disclosure, holding or otherwise general processing of data. APP entity is defined in section 6 of the Privacy Act to mean "an agency or organisation". "Agency" is further defined and mainly refers to a federal government entity and/or office holder. "Organisation" is further defined as including an individual, body corporate, partnership, unincorporated association, or trust that is not a small business operator (turnover of AU$3 million or less – although there are exceptions), a registered political party, an agency, a state or territory authority or a prescribed instrumentality of a State or Territory.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Personal data is referred to as "Personal Information" in the Privacy Act. Personal information is defined in section 6 as:

"Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not."

[36] Office of the Australian Information Commissioner, 'Global Privacy Expectations of the Libra Network' (Media Release, 6 August 2019). https://www.oaic.gov.au/updates/news-and-media/global-privacy-expectations-of-the-libra-network.

The Privacy Act places different types of personal information into further sub-categories:

- "sensitive information"; including "health information";
- "credit information" (further defined by the Privacy Act);
- "employee record" information; and
- "tax file number information".

Personal information that is "sensitive information" is subject to a higher threshold of data and privacy regulation, in comparison to other forms of personal data and information. Sensitive information is defined as:

- any information or opinion about an individual relating to one or more of the below characteristics:
    - Racial or ethnic origin; or
    - political opinions; or
    - membership of a political association; or
    - religious beliefs or affiliations; or
    - philosophical beliefs; or
    - membership of a professional or trade association; or
    - membership of a trade union; or
    - sexual orientation or practices; or
    - criminal record; that is also personal information;
- health information about an individual (further defined by the Privacy Act); or
- genetic information about an individual that is not otherwise health information (further defined by the Privacy Act); or
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

The Privacy Act makes a distinction between the ability of individuals to remain anonymous or pseudonymous in providing personal information to an APP entity and the de-identification of personal information held by an APP entity.

Australian Privacy Principle 2 provides that "Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP

entity in relation to a particular matter". Exceptions apply where "the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves" or "it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym".

The Privacy Act does not define "Anonymity" or "Pseudonymity". The OAIC provides the following guidance:

> Anonymity requires that an individual may deal with an APP entity without providing any personal information or identifiers. The entity should not be able to identify the individual at the time of the dealing or subsequently.

...

Pseudonymity requires that an individual may deal with an APP entity by using a name, term or descriptor that is different to the person's actual name. Examples include an email address that does not contain the person's actual name, a username that a person uses when participating in an online forum, or an artist who uses a "pen-name" or "screen-name".[37]

Further, Australian Privacy Principle 11 provides that an entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification, or disclosure. Under this principle, an APP entity must destroy or de-identify personal information in certain situations. Section 6 of the Privacy Act provides that personal information is de-identified "if the information is no longer about an identifiable individual or an individual who is reasonably identifiable."

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

There is currently no specific legislation in Australia regulating the use of blockchain technology. Australia has largely adopted a principles-based functional regulatory approach requiring applications of blockchain technology to comply with general legislative provisions such as the Privacy Act.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

The OAIC has provided high-level guidance on de-identification of data. The OAIC advises amongst other things that:

> There is no one "right" way to de-identify data. De-identification techniques should be carefully chosen, based on a risk assessment, to ensure that

[37] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (2019, Australian Government), p. 72. https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity.

> personal information is protected and that the information will still be useful for its intended purpose after the de-identification process.[38]

The OAIC, in conjunction with CSIRO's Data61, has published *The De-Identification Decision-Making Framework*.[39]

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

There is no general requirement under the Privacy Act to store personal information locally. Indeed, one of the objects of the Privacy Act listed in section 2A is to "facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected". Specific exceptions are made in other legislation and government policy. International transfers are governed by Australian Privacy Principle 8 in conjunction with section 16C of the Privacy Act.

Australian Privacy Principle 8 provides that:

> Before an APP entity discloses personal information about an individual to a person:
>
> (a) who is not in Australia or an external Territory; and
>
> (b) who is not the entity or the individual;
>
> the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

However, Australian Privacy Principle 8 will not apply where the organisation reasonably believes that the recipient of the information is subject to a law or binding scheme which provides for a level of protection that is similar to the Privacy Act, if the individual consents to the transfer (and consents to Australian Privacy Principle 8 not applying), such disclosure is required or authorised by law or by a court/tribunal order, or if another permitted general situation applies.

Section 16C provides that the disclosing and/or transferring entity will generally remain liable for any acts or omissions by the overseas recipient that would, if done by the disclosing organisation.

10. Is it necessary to notify processing activities to any authorities?

There is no legal requirement to notify processing activities to the privacy regulator. However, there are exceptions to this rule depending on the industry. For example, regulated organisations in the superannuation, banking and insurance industry may have reporting requirements. There are also reporting requirements for APP entities when personal information is accessed or disclosed without authorisation or is lost.

---

[38] Office of the Australian Information Commissioner, *De-identification and the Privacy Act* (2018, Australian Government), p. 11. https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act.
[39] Christine M O'Keefe et al. *The De-Identification Decision-Making Framework* (CSIRO Reports EP173122 and EP175702, 2017). https://publications.csiro.au/rpr/download?pid=csiro:EP173122&dsid=DS1.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

The Privacy Act provides protection for personal information of individuals – i.e., natural persons. The Australian Privacy Principles **(APP)** cover the following areas:

- APP 1 – open and transparent management of personal information;
- APP 2 – anonymity and pseudonymity;
- APP 3 – collection of solicited personal information;
- APP 4 – dealing with unsolicited personal information;
- APP 5 – notification of the collection of personal information;
- APP 6 – use or disclosure of personal information;
- APP 7 – direct marketing;
- APP 8 – cross-border disclosure of personal information;
- APP 9 – adoption, use or disclosure of government related identifiers;
- APP 10 – quality of personal information;
- APP 11 – security of personal information;
- APP 12 – access to personal information;
- APP 13 – correction of personal information.

It is important to note that there is no general right to privacy and there is no private enforcement of the APP obligations. This means that an aggrieved individual would need to make a complaint to the OAIC or bring other civil action (e.g., for breach of contract).

The right to be forgotten or to have personal data erased is not recognised in Australia.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

The Privacy Act applies to an "APP entity" (see above).

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The Privacy Act applies to an "APP entity" (see above).

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

Public blockchains have potential for preserving data privacy but also raise challenges in the open and transparent nature of the network and the inability to remove information added to public networks. One challenge is in the global nature of blockchain ecosystems and the requirement not only to comply with Australian privacy law but also to comply foreign regimes such as the GDPR. On the other hand, with public blockchains there may be no responsible entity that OAIC as regulator can act against. Another challenge exists in data that goes beyond the definition of "personal information" in the Privacy Act. For instance, data from corporate entities using blockchain applications may be commercially sensitive but are not covered by the Privacy Act (although there may be other avenues for legal recourse). For these reasons, it is important not to look at privacy legislation in isolation but also consider broader issues of cybersecurity, security, governance, and identity management – and at a multi-jurisdictional level.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

There is no established best practice, although it is noted that the work of standards bodies and other governmental efforts is continuing. For example, Standards Australia released a Roadmap for Blockchain Standards in 2017 which highlighted the need for continued work on privacy, security, and identity issues.[40] In addition, Australia's National Blockchain Roadmap in 2020 noted the continuing work of, and Australia's leadership in, the International Standardization Organization Technical Committee 307 – Blockchain and Distributed Ledger Technologies, which have a working group on security, privacy and identity.[41]

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

The *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 is the relevant AML legislation in Australia. AUSTRAC is the Australian regulator responsible for AML/CTF. The Financial Action Task Force **(FATF)** "travel rule" is not yet fully implemented or recognised within Australian legislation.

The Senate Select Committee on Australia as a Technology and Financial Centre examined this issue in its recent inquiry (2020–2021). The issue is contentious with the Committee noting that "submitters expressed concern that if the travel rule

[40] Standards Australia, 'Roadmap for Blockchain Standards' (Report, 2017).' https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx.

[41] Department of Industry, Science, Energy and Resources, 'The National Blockchain Roadmap' (Report, 2020). https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf.

were implemented in a strict way in Australia, this would create significant damage to the digital assets sector".[42] Ultimately the Committee recommended that:

> "The Anti-Money Laundering and Counter Terrorism Financing regulations be clarified to ensure they are fit for purpose, do not undermine innovation and give consideration to the driver of the Financial Action Task Force 'travel rule'."[43]

The Federal government noted this recommendation in its response to the Senate Committee and stated:

> Home Affairs and AUSTRAC will continue to proactively engage with industry and global partners to understand the challenges associated with implementing the FATF Standards, including the travel rule, and will ensure that any future legislative reforms are fit for purpose and meet the underlying objectives and drivers of the FATF Standards.[44]

[42] Senate Select Committee on Australia as a Technology as Financial Centre, 'Final Report' (Report, 2021), p. 59. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/AusTechFinCentre/Final_report.
[43] Ibid, recommendation 5.
[44] Treasury, 'Transforming Australia's Payment System' (Report, 2021), p. 12. https://treasury.gov.au/sites/default/files/2021-12/p2021-231824_1.pdf.

Brazil

Authors

Tatiana Campello, Demarest Advogados

Betina Portella Cunha Ferreira, Demarest Advogados

Julia Davet Pazos, DSMA Azulay

1. What are the legal acts regulating data privacy in your jurisdiction?

The main regulation is the General Personal Data Protection Law (Law No. 13,709/18 – LGPD), which became effective on 18 September 2020. The sanctions related to non-compliance with the LGPD started being applied from 1 August 2021, as provided for by Law 14,010/20.

More recently, on 28 October 2021, the ANPD approved the Regulation of the Supervision Process and the Sanctioning Administrative Process which aims to establish the procedures for surveillance, monitoring activities, guidance and preventive action, as well as to determine the rules to be observed on sanctions' application. It is worth noting that the ANPD has yet to determine the dosimetry of the sanctions and may issue other directives.

The Regulation stated that the ANPD plans to adopt educational and compliance measures before adopting more strict sanctions. However, depending on the conduct of the Controller, the gravity of the incident and the measures taken, the ANPD has the liberty to forego the educational steps and apply directly the sanctions.

The LGPD foresees the following administrative sanctions applicable for any non-compliance with the norms, which are cumulative: (i) warning, indicating the period for corrective action; (ii) a fine of up to 2 % of the income of the legal entity, group or conglomerate in Brazil in its last fiscal year, excluding taxes, limited in total to R$50,000,000.00 for each infraction; (iii) daily fine, observing the total limit of R$50,000,000.00 for each infraction; (iv) publicity of the infraction after duly verified and confirmed its occurrence; (v) blocking the personal data that the infraction refers to until its regularisation; and (vi) deletion of the personal data to which the infraction refers.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

The LGPD created the National Authority for Data Protection (ANPD). In general terms, the ANPD is responsible for:

- ensuring the protection of personal data;

- issuing rules and procedures regarding the protection of personal data and establishing norms that simplify procedures for micro- and small-sized businesses as well as for startups engaged in disruptive initiatives;
- deliberating, the interpretation of the LGPD, its competences and omissions on the administrative level;
- requesting information at any time from the controllers and processors of personal data;
- implementing simplified mechanisms for recording complaints about the processing of personal data not in accordance with the LGPD;
- supervising and applying sanctions in cases of non-compliance; and
- promoting cooperative actions with data protection authorities of other countries.

Despite the provision for such an authority in law, the ANPD is still non-functional. Currently, there are also several public ministries investigating possible data leaks and imposing appropriate fines.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

We do not have any specific regulation, guidance or opinions issued regarding blockchains.

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

The LGPD mentions the following actors:

- “Data subjects” are individuals to whom personal data belongs;
- “Controller” means a natural or legal person who is responsible for decisions on the processing of personal data;
- “Processor” refers to a natural or legal person who performs data processing on behalf of the controller;
- “National Authority for Data Protection” is the federal public administration body, member of the Presidency of the Republic, responsible for overseeing, implementing and monitoring compliance with the LGPD;
- “Data Protection Officer” (DPO) is a natural or legal person, nominated by the controller and the processor in some circumstances, who acts as a communication channel between the controller, the personal data subjects and the National Authority.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

According to the LGPD, "personal data" refers to any information related to a natural person, identified or identifiable. The LGPD considers personal data to be that which is used to form the behavioural profile of a specific individual, provided that they can be identified.

The LGPD also defines "sensitive personal data" as personal data on racial or ethnic origin, religious beliefs, political opinions, membership to a trade union or religious organisation, philosophical or political conviction, data on health or sexual life, genetic or biometric data, when it is linked to a natural person.

Lastly, personal data that belong to children and teenagers are given special protection by the LGPD, such as the need for specific and highlighted consent given by at least one parent or legal guardian in order to process children's personal data.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

The LGPD defines anonymised data as any data relating to a data subject that cannot be identified using reasonable and available technical means at the time of data processing.

On the other hand, the LGPD defines pseudonymisation as the treatment by which data loses the possibility of direct or indirect association with an individual, if not possible through the use of additional information maintained separately by the controller in a controlled and safe environment.

Anonymised data is not considered personal data by the LGPD, except when the anonymisation process to which it was submitted is reversed using exclusively its own means, or when it can be reversed with reasonable efforts.

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

Currently, there is not any specific legislation regarding blockchain technology in Brazil. The Chamber of Deputies is currently discussing the need to regulate this technology.

It is important to mention that the Brazilian Civil Rights Framework for the Internet (Law 12.965/14) must also be observed, as it establishes guidelines for internet use in Brazil. The main goal of this law is to regulate the relationship between companies that operate products or services associated with the internet and their respective users within the national territory.

It is also worth mentioning that this law assigns the duty of confidentiality of information to the internet resource provider. A breach of such guarantee can only occur by means of a court order, when such information is essential for the verification of illegal actions, as well as in an attempt to identify those responsible for such actions.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

As of this report's publication, no anonymisation or pseudonymisation techniques have been addressed by the data privacy authority.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

The LGPD does not require that personal data be stored in Brazil. However, the transfer of personal data to other countries will only be permitted when one of the following cases occur:

- The receiving country or international organisation provides a degree of protection adequate to that provided for in the LGPD;
- The controller proves compliance with the principles of the LGPD, data subject rights and protection regime;
- Transfer is necessary for international legal cooperation;
- Transfer is necessary for the protection of the life or physical safety of the subject or third party;
- The National Authority authorises the transfer;
- The transfer results in a commitment made in an international cooperation agreement;
- Transfer is necessary for execution of public policy or legal allocation of public service;
- The data subject has given their specific and express consent for the transfer; or
- Transfer is necessary to (a) meet a legal or regulatory obligation by the controller; (b) the execution of contract or preliminary procedures; or (c) the regular exercise of rights in judicial, administrative or arbitral proceedings.

10. Is it necessary to notify processing activities to any authorities?

The LGPD does not require notification of processing activities to the National Authority. However, the controller and the processor must keep a record of the personal data processing operations they carry out, especially when based on legitimate interest.

The ANPD may order the controller to prepare an impact report on the protection of personal data, including sensitive data, relating to its data processing operations. This report shall contain, at least, a description of the types of data collected, the methodology used for the collection and to guarantee the security

of the information and the analysis of the controller in relation to the measures, safeguards and risk mitigation mechanisms adopted.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

The data subjects have the following rights according to the LGPD:

- Confirmation of the existence of data processing activity.
- Easy access to the processing in a clear, adequate and explicit manner, explaining the purpose, form, duration of processing, identification of the party/parties responsible and their contact information, and the shared use of the personal data.
- Access to stored data.
- Correction of incomplete, inaccurate or outdated data.
- Anonymisation, blocking or elimination of unnecessary, excessive or processed data not in compliance with the provisions of the LGPD.
- Data portability to another service or product provider, upon express request.
- Information of the public and private entities with which the controller shared the data.
- Withdrawal of consent, except in cases determined by the law.
- Preservation and inviolability of the freedom, privacy and intimacy of the data subjects.
- Prerogative of not giving consent for processing and being informed of the consequence of such refusal.

There are strong discussions about the right to be forgotten in Brazil, especially relating to the nomenclature itself. Many doctrines defend the existence of the "right to deindexation" and other rights to the detriment of the right to be forgotten. There are a lot of doctrine and jurisprudential discussions, but we still do not have something positive or consensual in Brazil.

It is also important bearing in mind that there is a controversy relating to some impasses between blockchains and the LGPD. This is because the LGPD determines that the data subject has the right to request that the data is erased/deleted; however, blockchain is a technology known for the inability of data erasing. Bearing this in mind, even though we have not expressed a right to be forgotten, it is worth emphasising that we have a right to the elimination/deletion of data in LGPD, which is a sensitive discussion in regard to blockchain technology.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

The LGPD only holds the data controller and processor responsible for the breach of personal data. There is joint liability of the processor when it fails to comply with the law or the lawful orders of the controller. That is, both are responsible for the damage caused. However, if the processor can prove that the damages were caused by acts carried out by the controller, it will have the right of recourse, allowing the processor to be reimbursed by the controller for all the amounts it has disbursed to compensate the damages of the data subjects affected. The same rationale applies if the controller proves that the damage has been caused by the processor.

Processing agents will not be liable when they prove that: (i) they did not perform the activity assigned to them or (ii) the fault lies exclusively with the data subject or third parties.

It is important to mention, as the ANPD is still not acting in Brazil, we do not know how this Agency will regulate blockchain actors, such as miners, and if they will be considered as controllers or processors.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The LGPD will be applicable to private and permissioned blockchains, regardless of the country of its headquarters or the country where the data is located, when:

1) the processing of the operation is carried out within the national territory;

2) the processing activity has the objective of offering or providing goods or services or processing data from individuals located in the national territory; or

3) the personal data that is subject to processing has been collected within the national territory.

However, as already mentioned, the LGPD will not be applicable to anonymised data, except when the anonymisation process to which it was submitted is reversed, using exclusively its own means, or when, with reasonable efforts, it can be reversed.

The Brazilian Civil Rights Framework for the Internet (Law 12.965/14) must also be observed as it establishes guidelines for internet use in Brazil. The main goal of this Law is to regulate the relationship between companies that operate products or services associated with the internet and their respective users within the national territory.

It is worth mentioning that this Law assigns the duty of confidentiality of information to the internet resource provider. The breach of this guarantee can only happen by means of a court order, when such information is essential for the

verification of illegal actions, as well as in the attempt to identify those responsible for such actions.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

Firstly, it is important to highlight that current data protection laws have not considered decentralised technology in their provisions, and in Brazil there is no specific regulation on blockchain yet.

In any case, some issues may arise such as determining the legal basis on which personal data is processed, this complexity is due to the many actors involved, as well as the lack of direct relationship between actors and the data processing part.

Also, satisfying the rights of data subjects, such as the right to rectify data upon request, which can be a challenge in public blockchains designed to provide immutability.

Besides this, there are also challenges regarding the category of data and data subjects involved, for example, the processing of sensitive data or minors data can be considered of high risk. As well as information regarding the business structure, consumers and suppliers.

In this sense, the controller should be in compliance and take into consideration whether a public blockchain would be the best choice on a case-by-case analysis.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

As Brazil does not have a specific regulation yet, the LGPD and other applicable laws should be taken into consideration.

In order to be compliant, companies should assess to which jurisdictions its business model is subject, and whether the data covered by it meets the definition of personal and sensitive data under the jurisdiction of a particular data protection law in order to take the appropriate measures.

It should also establish the responsibilities of controllers and processors involved through Data Processing and Transfer Agreements, establish privacy policies and other related documents. As well as it should establish means of communication for the data subjects and when possible anonymise personal data or reconsider where and how it is stored.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

In Brazil, transactions with cryptocurrencies are already supervised by Normative Instruction No. 1,888/2019. This norm obliges platforms that trade digital currencies to declare their movements on a monthly basis about the transactions carried out by their clients. That is, data such as the data subjects involved in the transaction, the amount of crypto assets, the value of the transaction, and the amount of possible service fees must be reported to the Brazilian tax authority, under penalty of a fine. The “travel-rule” is, in a way, already being followed by Brazil.

In any case, this and many FATF recommendations are being discussed by the Brazilian Senate Committee, which is about to approve the “Marco das Criptomoedas” (Cryptocurrency Framework).

The Cryptocurrency Framework, “PL 2303/15”, establishes criteria for companies in the category of cryptoactive brokerage houses (or "exchanges") and lists a series of duties and conditions that this type of company will be required to comply with.

Companies linked to this market will also have to share more information with government agencies and will have six months to adapt to the new rules. It also creates a supervisory body, to be appointed by the Executive Branch, which will be responsible for authorising and controlling the operation of cryptoactive exchanges.

Canada

Authors

Luca Lucarini, Dentons

Chloe Snider, Dentons

Noah Walters, Dentons

1. What are the legal acts regulating data privacy in your jurisdiction?

Bill C-11 is still being debated at the time of writing.

In Canada, privacy is regulated by federal and provincial (or territorial) legislation and by certain common law principles. These various statutes and common law principles govern the collection, use and disclosure of personal information in both public and private sector activities in Canada.

The Federal Privacy Act applies to the federal government's collection, use, disclosure, retention or disposal of personal information in the course of providing services. It applies to various federal government institutions. This act also addresses individuals' ability to access and correct personal information held by the government of Canada.

The Federal Personal Information Protection and Electronic Documents Act (PIPEDA) governs the collection, use and disclosure of personal information of employees of federally regulated businesses like airlines, banks, railways, telecommunications companies and internet service providers regardless of where the activities take place.

More generally, it applies to all businesses that operate in Canada and collect personal information that crosses provincial or national borders in the course of commercial activities. The provinces of Alberta, British Columbia and Quebec have privacy statutes that are substantially similar to PIPEDA: Alberta's Personal Information Protection Act, British Columbia's Personal Information Protection Act and Québec's An Act Respecting the Protection of Personal Information in the Private Sector.

At the provincial level, there are various statutes that govern the collection, use and disclosure of personal information by the provincial and territorial governments, as well as the collection, use and disclosure of personal health information. For example, in Ontario, the Freedom of Information and Protection of Privacy Act regulates the collection of personal information by the Ontario government, the Municipal Freedom of Information and Protection of Privacy Act regulates the collection of personal information by municipal governments and the Personal Health Information Protection Act of 2004 regulates the collection of personal health information in Ontario.

Determining which data protection laws apply depends on the (1) nature of the organisation handling the personal information, (2) where the organisation is based, (3) what type of information is involved and (4) whether the information crosses provincial or national borders. In Canada, lawmakers are also developing common law that imposes civil liability for certain types of privacy breaches.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

The federal, provincial and territorial branches of government each have a designated privacy commissioner that reports to its respective legislature and oversees compliance with the applicable data protection regulations in its jurisdiction. For personal information collected in the course of commercial activities, the Office of the Privacy Commissioner of Canada (the OPC) would most commonly be designated as the relevant regulator.

The Federal Competition Bureau has also taken enforcement steps regulating the accuracy of privacy policies.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

Canadian privacy commissioners have not issued specific regulation, guidance or opinions on blockchain.

The only statements by the OPC to date on blockchain related technology is its joint statement on Facebook's Libra[45] that identifies issues arising from the transmission of data on the Libra network, a transmission process facilitated using blockchain technology. The statement raised the following issues:

- How will the network ensure that data protection standards, policies and controls apply consistently across jurisdictions;
- How will the organisation ensure that all processors within the network are identified and compliant with their jurisdictions' data protection laws;
- Where data is shared, to what extent will it be de-identified, what method of de-identification will be used, and how will the organisation ensure that data is not re-identified.

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

In the context of regulating privacy in the private sector, Canadian privacy laws generally apply to "organisations" as that term is defined in the relevant statutes, each of which provides a slightly different definition. All of the definitions are, however, broad in their scope.

[45] Full statement: https://www.priv.gc.ca/en/opc-news/speeches/2019/s-d_190805/.

Under PIPEDA, "organisations" are broadly defined to include "an association, a partnership, a person and a trade union". An organisation is responsible for personal information that it has transferred to a third party for processing and must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Under Alberta's Personal Information Protection Act, an "organisation" includes:

- a corporation,
- an unincorporated association,
- a trade union defined in the Labour Relations Code,
- a Partnership defined in the Partnership Act, and
- an individual acting in a commercial capacity, but does not include an individual acting in a personal or domestic capacity.

Under British Columbia's Personal Information Protection Act, an "organisation" includes "a person, an unincorporated association, a trade union, a trust or a not for profit organisation", but does not include:

- an individual acting in a personal or domestic capacity or acting as an employee,
- a public body,
- the Provincial Court, the Supreme Court or the Court of Appeal.

Under these statutes, the data subjects are generally individuals (meaning natural persons).

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

"Personal information" is defined in PIPEDA as "information about an identifiable individual". Generally, information that is considered to pertain to an identifiable individual is information which on its own, or combined with other pieces of data, can be used to identify a subject as an individual.

The OPC has stated that the following is considered personal information:[46]

- age, name, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

[46] Statement: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-andelectronic-documents-act-pipeda/pipeda_brief/.

Business contact information of an individual that an organisation collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession is not considered personal information.

The provincial personal health information statutes provide separate definitions for personal health information. For example, Ontario's 2004 Personal Health Information Protection Act, states that "personal health information" means identifying information about an individual in oral or recorded form, if the information relates, among other things, to the physical or mental health of the individual, the provision of health care to the individual, including the identification of a person as a provider of health care to the individual or the individual's health number.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

There are no express definitions for pseudonymous or anonymous data in Canadian privacy statutes.

However, the OPC has stated that anonymous information should not be considered personal information, "as long as it is not possible to link that data back to an identifiable person".[47]

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

While there is no blockchain specific legislation in Canada, the distinct federal, provincial, private, public and sector-specific privacy statutes may impact an organisation's use of blockchain technology. This will depend on the nature of the organisation and the manner in which blockchain technology is implemented to collect, use, disclose or store personal information.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

Neither the OPC nor any provincial privacy regulations has yet issued specific guidance about which rules and techniques they will use to address de-identification. However, the OPC (The Office of the Privacy Commissioner) in Canada has recognised that there are increasingly sophisticated means to re-identify information that ostensibly appears to be non-personal. In its Proposals to modernise the Personal Information Protection and Electronic Documents Act, [48] the OPC has stated: "The idea that the anonymization of information, which would render such information outside the scope of privacy legislation, is practically attainable, is unlikely." In the blockchain context this has proven to be true with Bitcoin, which many originally believed to be anonymous, and more

[47] www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.
[48] See https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

recently with Monero, where one study was able to uncover up to 85 % of sender identities (before the 2017 update).[49]

The proposed CPPA would provide some guidance to organisations on how to appropriately de-identify information. While specific requirements or techniques are not discussed, section 74 states: "An organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information." There is also a prohibition on using de-identified information, alone or in combination with other information, to identify an individual.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

In the public sector, only British Columbia and Nova Scotia require that all public sector data reside in Canada, while Ontario restricts only healthcare information. There are no private sector laws that require Canadian companies to store data within the country.

In response to COVID-19, British Columbia temporarily modified its Freedom of Information and Protection of Privacy Act to permit authorised health-care bodies to use communication and collaboration software that may host information outside of Canada. The order is subject to certain conditions and will remain in effect until 30 June 2020.

In the private sector, organisations are responsible for personal data transferred to third parties, including third-party processors outside of Canada. Generally, privacy statutes allow for the non-consensual transfer of personal information, provided that the transferring organisation provides a comparable level of protection to the information being processed internationally, albeit through contractual or other means.

In practice, Canadian organisations typically enter into an agreement when transferring data internationally for processing purposes to ensure that the standard of protection afforded by Canadian privacy statutes is met. Features of the agreement will likely depend on the size and context of the data transfer, and tend to consider security safeguards, contractual arrangements outlining requisite conditions, policies for notifying employees or consumers of data usage and possible breach and quality of oversight.

The OPC has recently looked more closely at related issues, suggesting organisations transferring personal information outside of Canada (including to a parent corporation) should consult with legal counsel to determine what steps should be taken in the circumstances.

10. Is it necessary to notify processing activities to any authorities?

Data transfers do not require prior registration, notification or approval from data protection authorities.

[49] See Malte Moser et al., "An Empirical Analysis of Traceability in the Monero Blockchain" (2017), arXiv 1704.04299, online: arxiv.org/pdf/1704.04299/ [Moser et al.].

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

In Canada, data subjects (individuals) generally have the following rights:

- Right of access to data:
    - Individuals have a right to be informed of the existence, use and disclosure of their personal information upon request, subject to limited exemptions. This right includes access to their information and requires the organisation processing the information to list third-party organisations with whom the information has been shared. The organisation must ensure the information is in a form that is understandable and respond to requests in a timely manner, at minimal or no cost to the individual. Exemptions to subjects' right to access vary between statutes. Examples of exemptions include, but are not limited to, confidential commercial information, information about another individual, information relating to national security, privileged information and information generated in a formal dispute resolution process.
- Right to rectification of errors:
    - Privacy laws generally require an organisation to correct inaccuracies or add a notation to the information when an individual identifies an error.
- Right to object to processing/right to restrict processing:
    - There is no explicit right to object or restrict processing in Canada. However, privacy laws generally prohibit organisations from requiring individuals to provide consent for collection, use or disclosure of their personal information as a condition for the use of a product or service beyond the personal information that is needed for the specified and legitimate purpose. An individual must otherwise have a choice as to whether to provide meaningful consent. For guidelines on the nature of consent organisations must obtain, and how they must obtain it, see the OPC's Guidelines for obtaining meaningful consent.[50]
- Right to withdraw consent:
    - Individuals are entitled to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Organisations must inform individuals of the implications of withdrawing consent upon receipt of a request.

[50] https://www.priv.gc.ca/en/privacy-topics/collective-personal-information/consent/gl_omc_201805/.

- Right to object to marketing:
    - Privacy laws require organisations to obtain consent from individuals for the collection, use and disclosure of personal information for marketing purposes.[51]
- Right to complain to the relevant data protection authorities:
    - Individuals must be able to address issues with the designated individual who is accountable for organisational compliance. Organisations must have policies and practices in place to receive complaints and must take steps to address complaints. Individuals also have the ability to complain to relevant data protection authorities.
    - Canadian privacy law does not include an explicit right to be forgotten that allows an individual to demand the deletion or erasure of their personal information. The most comparable rights in Canada are the right to withdraw consent, and challenge the accuracy, completeness and currency of personal data.
    - In a 2018 Reference to the Federal Court of Canada, the issue of de-indexing caused many to ask whether Canadians would soon have a right to be forgotten. The Federal Court decided that the Reference was not a suitable place for this debate; however, discussions about a right to be forgotten are ongoing, and there will likely be public consultations moving forward.[52]

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

Canadian privacy statutes and case law have not addressed the issue of accountability in public permissionless blockchain networks. Designating accountability for public permissionless blockchain privacy infringement is a difficult task because public permissionless blockchains are not owned by a single entity. Rather, the ownership, and ultimately the ability to exercise control over public permissionless blockchains becomes increasingly decentralised over time.

On public permissionless blockchain networks, there can be a centralisation of control by certain more powerful entities. These powerful entities are often composed of the core developers for the public permissionless blockchain network. Core developers set the rules that govern the blockchain, and in many cases, they are the individuals who handle the maintenance of the network during its development.

Accordingly, it is possible that such core developers may come within the definition of "organisation" under Canadian privacy legislation where they are collecting, using or disclosing personal information in Canada, so long as they are the primary arbiters for decisions related to the governance, maintenance and

[51] Ibid.
[52] Reference re: subsection 18.3(1) of the Federal Courts Act under subsection 18.3(1).

development of the public permissionless blockchain network and are collecting, using or disclosing personal information on the relevant platform.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The nature in which data privacy legislation applies to private and permissioned blockchains will likely depend on the nature of the organisation, and the manner in which blockchain technology is implemented to collect, use, disclose or store personal information.

In Gordon v. Canada (Health), 2008 FC 258, the Federal Court of Canada held that information is about an identifiable individual if it "permits" or "leads" to the possible identification of the individual, whether on the basis of that information alone, or when the information is combined with other information from other available sources.[53]

Accordingly, businesses that conduct transactions atop blockchain infrastructure will likely need to comply with PIPEDA (where it would otherwise apply) because the metadata engrained in private and permissioned blockchain transactions may constitute personal information. While context dependent, metadata will likely constitute personal information in the case of private and permissioned blockchain transactions because it may "lead" to or "permit" the determination of where transactions are sent from, who they are sent to (not necessarily the name of the recipient, but the address), how much money was sent and at what time, which would constitute personal information.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

Due to the lack of blockchain specific legislation in Canada, there are no specific legal limits on the use, transfer, and storage of data when public blockchains are used. However, PIPEDA imposes general legal limits on the use, transfer, and storage of data by private sector organisations. Pursuant to section 5 of PIPEDA, every organisation must comply with the 10 principles set out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information. Accordingly, the following legal limits apply to private organisations:

- Organisations must identify the purposes for which personal data is being collected before or at the time of collection.
- Individuals' consent is generally needed for the collection, use or disclosure of personal information.
- Information must be collected by fair and lawful means and must be limited to the data needed for the purpose identified by the organisation.

[53] Office of the Privacy Commissioner of Canada, Metadata and Privacy: A Technical and Legal Overview (Gatineau, Q.C.: Office of the Privacy Commissioner of Canada, October 2014) at 6, online: www.priv.gc.ca/media/1786/md_201410_e.pdf).

- Personal information can only be used or disclosed for the purposes for which it was collected and must be kept solely for the duration required to serve those purposes unless the individual consent otherwise or it is required by law.

- Personal information must be protected through appropriate security safeguards against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification.

- Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to it.

It is likely that the above listed limitations imposed by PIPEDA will also apply in the public blockchain context.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

No official recommendations or interpretations of how to process personal data on public or private blockchains have been published in Canada. However, a broad interpretation of personal information, which is customary under Canadian laws, could deter blockchain stakeholders from processing personal data on public blockchains because data on a blockchain is accessible by anyone with access to that blockchain, and distributed/stored amongst all nodes in the public blockchain network. Ultimately, blockchain features of accessibility, immutability and decentralisation (of storage and processing) make it difficult to accommodate the rights of data subjects related to use, disclosure, collection and consent.

In the private blockchain context, management of individual rights over personal information is possible because there are designated and accountable entities that control the number of stakeholders with access to the blockchain. Under such circumstances stakeholders may require compliance with privacy regulations as a means of accessing the private blockchain and its associated application(s). Stakeholders may also be removed from the network for failures to comply, and a sufficiently centralised private blockchain may be overwritten by participants through collaboration to respond to certain privacy infringing incidents.

For either public or private blockchain use cases that involve personal data, organisations should adopt best practices that involve:

- Combining on chain and off chain data
    - The blockchain application should avoid storing personal data as a payload on the blockchain (i.e., including identifying information in the message accompanying the payment itself), and instead have blockchain transactions serve as mere pointers or an access control mechanism to more readily managed storage solutions off-chain.

- Utilising privacy centric technologies and cryptographic methods
    - Encryption techniques currently being used by privacy centric chains include ZK-SNARKS, Ring Confidential Transactions, and mixing techniques, all of which are intended to mask the identify of the sender or recipient and/or allow participants to confirm transactional legitimacy by cryptographically proving that they know something without revealing the nature and identity of the information.
    - These privacy-friendly techniques may run into additional regulatory concerns, especially for cryptocurrencies or other financial transactions, including know your customer, anti-money laundering, and anti-terrorism laws and regulations.
    - Other privacy enhancing encryption and destruction techniques may be used to protect an individuals privacy rights, such as hashing data or applying other data transformation techniques to personal information and revocation of access rights to a blockchain application (or entire blockchain in a private blockchain network). However, Canadian regulators have not addressed whether such measures are sufficient to meet the demands of Canadian privacy legislation.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

The “travel-rule” has been implemented into Canada’s AML legislation through the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (“PCMLTFA”) and its regulations. The travel rule requires specific information to be included with the information sent or received in a virtual currency (“VC”) transfer.

Financial entities, money services businesses, foreign money services businesses must include the following information when they send VC transfers, and must take reasonable measures to ensure that this information is included when they receive VC transfers which require a VC record to be kept (i.e., when transferring or receiving US$1,000 or more in VC):

- the name, address and the account number or other reference number (if any) of the person or entity who requested the transfer (originator information); and
- the name, address and the account number or other reference number (if any) of the beneficiary.

If a VASP receives a VC transfer that should include the travel rule information but does not, it is their responsibility to take reasonable measures to obtain that information. These reasonable measures should be outlined in your policies and procedures.

China

Author

Hu Ke, Jingtian & Gongcheng

Yuan Lizhi, Jingtian & Gongcheng

1. What are the legal acts regulating data privacy in your jurisdiction?

There are various laws, departmental rules and national standards that serve to protect personal information in China. Under the Chinese legal system, the promulgating agencies and enforceability of laws, regulations and national standards are as follows:

1) Laws are promulgated by the legislative body, namely the National People's Congress (the "**NPC**") and its Standing Committee (the "**SCNPC**"). Laws are mandatory, and any regulations, national standards or regulatory requirements shall not conflict with laws.

2) Regulations are generally formulated or promulgated by administrative agencies. Many government agencies are involved in formulation and promulgation of regulations on personal information protection, including the Cyberspace Administration of China (the "**CAC**"), the Ministry of Industry and Information Technology (the "**MIIT**"), the Ministry of Public Security (the "**MPS**"), the State Administration for Market Regulation (the "**SAMR**"), the People's Bank of China (the "**PBC**"). Regulations also have a mandatory effect. Although the level of legal force of regulations is lower than that of laws, regulations have a higher level of legal force compared with national standards.

3) National standards are formulated and promulgated by the Standardization Administration of the People's Republic of China (the "**SAC**"). National standards are divided into mandatory national standards and recommended national standards. Mandatory national standards have a mandatory effect, while recommended national standards are not mandatory. The level of legal force of national standards is lower than that of regulations. Generally, the national standards on personal information protection are recommended national standards. Although the national standards on personal information protection do not have compulsory legal effect, they are also important references for regulatory agencies.

In terms of laws, in parallel with the Cybersecurity Law of the PRC (the "**CSL**"), the Data Security Law of the PRC (the "**DSL**") and the Personal Information Protection Law of the PRC (the "**PIPL**") were successively promulgated in 2021. These laws form a Chinese legal system for cybersecurity, data security and personal information protection. To be specific:

1) **The CSL:** On November 7, 2016, the SCNPC promulgated the CSL, which became effective on June 1, 2017. The CSL requires network operators to comply with laws and regulations and fulfil their obligations to safeguard security of the network when conducting business and providing services.

   The CSL provides that: (a) to collect and use personal information, network operators shall follow the principles of legitimacy, rightfulness and necessity, disclose rules of data collection and use, clearly express the purposes, means and scope of collecting and using the information, and obtain the consent of the persons whose data is gathered; (b) network operators shall neither gather personal information unrelated to the services they provide, nor gather or use personal information in violation of the provisions of laws and administrative regulations or the scopes of consent given by the persons whose data is gathered; and shall dispose of personal information they have saved in accordance with the provisions of laws and administrative regulations and agreements reached with users; (c) network operators shall not divulge, tamper with or damage the personal information they have collected, and shall not provide the personal information to others without the consent of the persons whose data is collected.

2) **The DSL:** On June 10, 2021, the SCNPC passed the DSL, which became effective as of September 1, 2021. The DSL is broadly applicable to and will impact all operators that engage in the processing of all types of data. The DSL shall apply to data processing activities and security supervision of such activities within the territory of the PRC; where data processing activities outside the territory of the PRC damage the national security, public interests or the legitimate rights and interests of citizens and organisations, it shall also be subject to the DSL.

   The DSL provides for data security and privacy obligations on entities and individuals carrying out data processing activities, introduces a data classification and hierarchical protection system based on the importance of data in economic and social development, as well as the degree of harm it will cause to national security, public interests, or legitimate rights and interests of individuals or organisations when such data is tampered with, destroyed, leaked, or illegally acquired or used, and provides for a national security review procedure for data activities that may affect national security and imposes export restrictions on certain data and information.

3) **The PIPL:** On August 20, 2021, the SCNPC passed the PIPL, which became effective on November 1, 2021. The PIPL is the first and most important special law focusing on the protection of personal information in China, which provides comprehensive protection for the rights and interests of personal information. The PIPL shall apply to the processing of the personal information of natural persons within the territory of the PRC; the PIPL shall also apply to the processing of the personal information of Chinese people outside the territory of the PRC when: (a) where the purpose is to provide Chinese people with products or services; (b) where the activities of Chinese

people are analysed and evaluated; and (c) other circumstances as prescribed by laws and regulations.

The PIPL accentuates the importance of personal information processors' obligations and responsibilities for personal information protection, and sets out the basic rules for processing personal information and the rules for cross-border transfer of personal information. The PIPL further supplements the existing data protection regime previously established by the CSL. Instead of relying only on "notification and consent" as established in the CSL, the PIPL expands the legal bases for processing personal information. Processors shall also take necessary measures to ensure the security of the personal information processed, and take specific measures to protect the personal information of children. The PIPL provides the rights of data subjects, including right to be informed, make decisions and require an explanation, right to restrict or refuse the processing, right of access and duplicate, right of portability, right of rectification and supplementation, right of erasure and deletion, right to cancel the account, right of withdrawal of consent, and right for close relatives of a dead person.

In terms of regulations, the provisions of personal information protection are mainly embodied in the regulations of a specific industry or a special field. To be specific:

1) In the telecommunications and internet sector, the MIIT promulgated the Provisions on Protecting the Personal Information of Telecommunications and Internet Users in 2013. This regulation provides for the rules on the collection and use of personal information by telecommunications business operators and internet information service providers, as well as the corresponding safety measures.

2) In the financial sector, the Implementation Measures for the Protection of Financial Consumer Rights and Interests promulgated by the PBC in 2016 and revised in 2020 requires financial institutions to obtain the express consent before collecting and using financial information of consumers, and also stipulates the scope of data collection, restrictions on the use of data for marketing, prohibition of discrimination, exercise of rights, and information security emergency management.

3) In the field of child protection, the CAC has promulgated the Provisions on Online Protection of Children's Personal Information in 2018 to regulate the protection of minors' personal information online under the age of 14.

4) In addition, China's regulatory authorities have paid particular attention to the field of mobile applications. In January 2019, the CAC, the MIIT, the MPS and the SAMR jointly launched a Special Crackdown Campaign against Illegal Collection and Use of Personal Information by Apps. In November 2019, the CAC, the MIIT, the MPS and the SAMR promulgated the Methods for Identifying the Illegal Collection and Use of Personal Information by Apps. In July 2020, the MIIT issued the Announcement on Launching In-depth Special Crackdown Campaign the Infringement of Users' Rights and Interests by Apps.

In terms of national standards, the "Information Security Technology – Personal Information Security Specification" (the "**PIS Specification**") was promulgated by the SAC in 2016 and amended in 2020. The PIS Specification stipulates the principles and security requirements of collection, storage, use, sharing, transfer, public disclosure and other processing activities of personal information. The PIS Specification plays an important role in personal information protection, which is an important standard for detailing and supporting the requirements for personal information protection as specified in the CSL.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

There is no unified personal information protection regulatory authority in China. Multiple government departments work in collaboration to jointly manage personal information protection. To some extent, responsibilities of various departments could overlap. According to the CSL, the CAC is responsible for the overall planning and coordination of cybersecurity, as well as the supervision and administration of relevant personal information protection. MIIT, MPS and other relevant authorities are responsible for the supervision and administration of cybersecurity and personal information protection within the scope of their respective duties in accordance with the CSL, relevant laws and regulations. The roles of the regulatory authorities are as follows:

1) **The CAC**: It is responsible for supervising personal information protection of network operators, and it also plays the role of overall coordination of personal information protection. The supervision method is to supervise the industry as a whole by promulgating policies, interviewing enterprises, and holding press conferences.

2) **The MPS**: It is responsible for preventing and punishing infringements of residents' personal information. The supervision method is to impose administrative penalties.

3) **The MIIT**: It is responsible for supervising and administering personal information protection in the management of network products and services. The supervision method is to promulgate relevant policies, interview enterprises, hold press conferences, and conduct special crackdown campaigns.

4) **The SAMR**: It is responsible for supervising and administrating the protection of the personal information of consumers. The supervision method includes issuing policies, holding press conferences, and administrative penalties (such as warning, publicity of illegal collection and uses, and fines).

In addition, the competent authorities of some industries will supervise and administrate personal information protection within the industry, such as the financial industry and the healthcare industry.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

At present, there is no specific law on blockchain in China. In terms of regulations, the only unified regulatory rules for the blockchain industry are the Administrative Provisions on Blockchain Information Services (the "**Blockchain Provisions**"). The Blockchain Provisions were released by the CAC in January 2019. The Blockchain Provisions require the blockchain information service providers to:

1) Fill in relevant information through the blockchain information service filing management system and perform filing procedures;

2) Perform the responsibilities for information content security management, and improve user registration, information review, emergency response, security protection and other management systems;

3) Possess the technical conditions suitable for the blockchain information services;

4) Enter into a service agreement with users of blockchain information services, specify the rights and obligations of both parties, and require them to undertake to comply with legal requirements and platform usage specification;

5) Authenticate the users' real identity information based on the organisation code, ID number or mobile phone number;

6) Report the development and launch of new products, new application or new functions to the CAC or provincial cyberspace administrations for security evaluation in accordance with relevant laws and rules;

7) Cooperate with the inspection by the supervisory authorities, and provide necessary technical support and assistance; and

8) Accept social supervision, set up convenient portals for complaints and reports, and handle public complaints and reports in a timely manner.

In addition, China has put a limitation on tokens in order to protect the status of RMB as the legal tender, and the regulations and industry self-discipline rules also reflect the limitation on tokens. The earliest regulatory document was the Notice on Precautions Against the Risks of Bitcoins (the "**Notice on Bitcoins**"), which was promulgated by the PBC and six other ministries in December 2013. The Notice on Bitcoins stipulates that financial institutions and payment institutions are not allowed to provide bitcoin-related services, and that websites providing bitcoins registration and transaction services shall be filed with telecommunication management authorities. In September 2017, the PBC and six other ministries released the Announcement on Preventing Risks relating to Fundraising through Token Offerings, requiring that all kinds of token fundraising activities shall be suspended, and that all the organisations and individuals that have already completed token fundraising should make arrangements such as returning funds. In January 2018, the Central Bank Payment and Settlement Department of PBC released the Notice on the Development of the Self-inspection and Rectification of

the Payment Service Provided for Illegal Virtual Currency Transactions, prohibiting financial institutions and payment institutions from providing services for virtual currency transactions or providing payment channels for virtual currency transactions.

In addition to tokens, the Chinese government is supportive of blockchain technology. The China government has enacted a series of policies and measures to encourage the development of blockchain technologies, so as to guide the application of blockchain technologies in the industry and promote industrial development. In December 2016, the State Council promulgated the "13th Five-year Plan for National Informatization (2016–2020)". The State Council is the highest administrative body in China. This is the first time that the Chinese government endorses blockchain technology as a strategic frontier technology encouraged by the country. As of January 2017, several departments of the State Council have issued policy documents supporting the development of blockchain technology. For example, the Ministry of Commerce issued the Guiding Opinions on Further Promoting the Construction of National E-commerce Demonstration Bases in January 2017 to promote the incubation of blockchain entrepreneurial bases. In January 2017, the Development Plan for Software and Information Technology Service Industry (2016–2020) issued by the MIIT required that the innovation in blockchain shall reach the internationally-advanced level. In December 2017, the PBC issued the "13th Five-Year Development Plan for the Information Technology for the PRC Financial Sector", specifying that it is imperative to strengthen the research of blockchain basic technologies and carry out the application of blockchain technologies in the financial sector. The CAC and the MIIT issued the Guidance on Accelerating the Promotion of Blockchain Technology Application and Industrial Development in May 2021, which states that blockchain should play an important role in industrial transformation.

Furthermore, in September 2021, the National Development and Reform Commission (the "**NDRC**") and other ten governmental departments jointly circulated the Notice on Regulating Virtual Currency "Mining" Activities, prohibiting mining activities for carbon neutrality. Under the Notice, it is required to sort out and investigate existing virtual currency "mining" projects and new projects under construction, and a strict ban is imposed on investment and construction of new "mining" projects. The government would also take measures to speed up the process of having existing projects exit the market in an orderly manner.

In the same month, the People's Bank of China (the "**PBOC**"), together with nine other governmental departments, jointly issued the Notice on Further Preventing and Resolving the Risks of Virtual Currency Trading and Speculation. The Notice clarifies that virtual currencies do not possess the same legal status as legal currencies, thus cannot be circulated in the market. All virtual currency-related businesses are classified as illegal financial activities according to the Notice. Moreover, it is considered illegal for overseas virtual currency exchanges to provide services to Chinese domestic residents via the Internet. The Notice warns that there are legal risks associated with virtual currency investment and trading. It is reiterated in the Notice that financial institutions and non-bank payment institutions are prohibited from providing services for virtual currency-related business activities.

4. What kind of actors (e.g., data subjects, controllers, processors...) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

In Chinese Laws, the CSL stipulates that "network operators" bear primary responsibilities for personal information protection. According to Art. 76 of the CSL, "network operators" are the owners and managers of the networks or network service providers thereon. The "networks" are systems composed of computers or other information terminals and related equipment which collect, store, transmit, exchange and process information in accordance with certain rules and procedures. "Network operators" are owners and managers of networks and service providers relying on the systems of the network.

According to the PIS Specification and relevant practice of data law, network operators could be grouped into the following three types:

1) **Personal Information Controllers**: In accordance with Art. 3.4 of the PIS Specification, a "personal information controller" is an organisation or individual with the ability to determine the purpose and method of the processing of personal information. This concept is similar to that of "data controller" under the EU General Data Protection Regulation (the "**GDPR**").

2) **Entrusted Processors**: The concept of "entrusted processor" under Art. 9.1 of the PIS Specification is derived from the concept of "processor" under the GDPR and must be understood vis-à-vis the concept of data controller.

3) **Technical Service Providers**: In addition to personal information controller and entrusted processor, there is another type of network operators that neither determine the purpose and method of data processing, nor is entrusted by others to process data; instead, they only provide the environment, facilities, and corresponding technical capabilities for data processing activities. They may be called "technical service providers", which include basic cloud service providers, telecommunications operators, etc.

However, the Civil Code, which came into effect on January 1, 2021, does not adopt the concept of "personal information controller" under the PIS Specification. Instead, the Civil Code adopts the concept of "information processor" to refer to "controllers".

The PIPL, when following the terminology in the Civil Code, further adopts the concept of "processors" under the Civil Code. The PIPL defines the personal information controller as the "personal information processor" and defines the entrusted processor as the "entrusted party" to cover those who process personal information without power to determine the processing activities. To be specific:

1) **Personal Information Processor**: Pursuant to Art. 73 of the PIPL, "personal information processor" refers to an organisation or individual that independently determines the purpose and method of the processing in the processing of personal information. It is a core concept and often the starting point for legal analysis under the PIPL, since a series of obligations

and responsibilities under the PIPL are carried out around the personal information processor.

2) **Entrusted Party**: Pursuant to Art. 21 of the PIPL, "entrusted party" refers to an organisation or individual processes personal information on behalf of a personal information processor. There is a principal-agency relationship between a personal information processor and an entrusted party.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Chinese laws and rules initially define personal information as information that identifies a person. For example, Art. 4 of the Provisions on Protecting the Personal Information of Telecommunications and Internet Users in 2013 provides that "personal information of users refers to the information collected by telecommunications service operators and internet information service providers in the process of providing services, such as the names, dates of birth, ID numbers, addresses, phone numbers, account numbers and passwords of users, which can be used to identify the users either independently or in combination with other information about when and where the users of use the services." Art. 76 item 5 of the CSL also provides that "personal information refers to various information recorded electronically or otherwise that can identify the personal identity of a natural person alone or in combination with other information."

Later, the definition of personal information took two approaches. In addition to "identification", it also includes "association". The "association" approach is to know a given individual and know about the individual's further information. According to the Supreme People's Procuratorate Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information promulgated in 2017, residents' personal information refers to various information recorded electronically or otherwise, which can be used, independently or together with other information, to identify the identity of particular natural persons or reflect the situation of their activities. According to Art. 3.1 of the PIS Specifications promulgated in 2016 and revised in 2020, personal information refers to "all kinds of information recorded by electronically or otherwise, which can, independently or in combination with other information, identify the identity of specific natural persons or reflect the activities of specific natural persons." Art. 4 of the PIPL stipulated that personal information shall refer to a variety of information related to an identified or identifiable natural person that is recorded electronically or otherwise, excluding anonymised information.

As for personal information classification, some industrial regulatory authorities in China have made some attempts in this regard. For example, in February 2020, the MIIT promulgated the Data Classification Guidelines for Securities and Futures Industry and the Industrial Data Classification Guidelines. In December 2021, the National Information Security Standardization Technical Committee has promulgated the Network Security Standard Practice Guidelines – Guidelines for Classification and Classification of Network Data. However, there is no uniform classification standard on personal information.

According to the PIPL, personal information is classified into general personal information and personal sensitive information. Specifically:

1) **Personal Sensitive Information:** Pursuant to Art. 28 of the PIPL, sensitive personal information shall the personal information that is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety once disclosed or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial account and whereabouts and tracks, as well as the personal information of minors under the age of 14.

2) **General Personal Information:** General personal information is personal information that does not belong to personal sensitive information.

According to the PIS Specification, personal biometric information is a special type of personal sensitive information. The PIS Specification does not explicitly define personal biometric information, but lists individuals' genes, fingerprints, voice prints, palm prints, auricles, irises, facial identification features as personal biometric information. The processing of personal biometric information shall be subject to more strict requirements than those applicable to the processing of personal sensitive information.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

The PIPL defines anonymisation and de-identification, but does not define pseudonymisation. The definitions of anonymisation and de-identification are as follows:

1) **Anonymisation**: According to Art. 73 of the PIPL, anonymisation refers to the process of processing personal information to make it impossible to identify specific natural persons and impossible to restore.

2) **De-identification**: According to the English version of PIPL published by NPC, pseudonymisation is called de-identification. Art. 73 of the PIPL stipulated that de-identification refers to processing personal information to make it impossible to identify specific natural persons in the absence of the support of additional information.

Anonymisation and pseudonymisation are defined in the national standards, and the definition of anonymisation under the national standards is similar to that under the PIPL. To be specific:

1) **Anonymisation**: According to Art. 3.14 of the PIS Specification, anonymisation is an irreversible technical process that makes personal information subjects unidentifiable or unassociated. Anonymised personal information is not to be deemed as personal information.

2) **Pseudonymisation**: According to Annex A Section 4.1 of the Information Security Technology – Guidelines for De-Identifying Personal Information, pseudonymisation technology is a de-identification technology that

replaces direct identification (or other quasi-identifier) with pseudonyms. The pseudonymisation technology creates a unique identifier for each personal information subject to replace the original direct-identifier or quasi-identifier. Related records in different data sets can still be correlated after pseudonymisation, and the identity of the personal information subject will not be revealed. According to Art. 3.15 of the PIS Specification, pseudonymised data is used as de-identified information, and because it can be combined with other information to re-identify or associate individuals, the pseudonymised data is still personal information.

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

Under the Chinese regulatory regime, the ledger layer, the consensus layer, and the smart contract layer of the blockchain system are the technical layers that are obviously different from other software solutions. To be specific:

1) In 2019, the "Blockchain White Paper (2019)" issued by China Academy of Information and Communication Technology sets forth a general technical framework for blockchain systems, under which the blockchain systems are divided into nine layers, namely infrastructure, basic components, ledgers, consensus, smart contracts, interfaces, applications, operation and maintenance, and system management.

2) In 2020, the Financial Distributed Ledger Technology Security Specification (the "**Financial DLT Specification**") was promulgated by the PBC, under which blockchain systems are divided into layers of smart contracts, consensus, ledger, node communication, basic software, basic hardware, and cryptography.

3) In 2021, the National Information Security Standardization Technical Committee promulgated the draft of Information Security Technology-Security Framework for Blockchain Technology (the "**Security Framework for Blockchain**"). Under this document, the blockchain systems are divided into layers of user, service interface, core function and fundamental infrastructure. The core function layer is the technical layer that is obviously different from other software solutions, and this layer includes functions of consensus, smart contracts, ledge and cryptography.

The laws and regulations in China do not mention the regulatory requirements of the ledger layer, the consensus layer, and the smart contract layer, and these technical layers are only regulated under the Financial DLT Specification and the Security Framework for Blockchain. To be specific:

1) **The Ledger Layer**: The structure of the ledger shall be tamper-proof, and hash nesting algorithm shall be used to ensure that the data is difficult to tamper with. The ledger layer shall have a data verification function. The integrity, consistency, confidentiality, validity and redundancy of the ledger shall be guaranteed, and access and use of the ledger shall meet security audit requirements.

2) **The Consensus Layer**: The consensus module shall be able to coordinate the orderly participation of all system participants in the data packaging and consensus process, and ensure the data consistency of all participants. When the system has no failure or fraud nodes, the consensus layer shall be able to reach a unanimous and correct consensus within the required time and output the correct results. The system shall operate correctly under the circumstance that the total number of failure nodes and fraud nodes do not exceed the theoretical limit. Furthermore, the consensus module shall select an appropriate consensus protocol.

3) **The Smart Contract Layer**: The version of the smart contract shall be defined in the source code, configuration files, deployment and upgrade, and the previous versions shall be retained after the upgrade. The version of the smart contract shall be specified in the transaction. Corresponding mechanisms shall be adopted to control users' access to the smart contract, limit erroneous infection, and visit the external environment. Smart contracts shall limit complexity, have atomic nature and consistency in execution, be audited and recorded, meet lifecycle management requirements, have attack prevention mechanisms, and pass security verification.

In addition, blockchain uses cryptography to ensure the security of transmission and access. Regarding cryptographic algorithms, Chinese laws and regulations stipulate as follows:

1) In October 2019, the SCNPC promulgated the Cryptography Law, which stipulates the definition of cryptography, basic principles of cryptography work, classification management system for cryptography and other important contents. Commercial encryption is most commonly used in the application of blockchains, and commercial encryption is required to follow laws, regulations, mandatory national standards, and industry technical standards. The commercial encryption products, which involve national security, national economy, people's livelihood, social interests and public interests, shall be listed in the catalogue of critical network equipment and cybersecurity products.

2) In December 2019, the SAMR and the State Cryptography Administration released the Notice Regarding Adjustment of Regulatory Approach for Commercial Encryption Products and abolished the Commercial Encryption Products Type and Model Certificate, establishing a nationally unified commercial encryption certification system, and encouraging commercial encryption products to obtain the certification.

3) In April 2020, the CAC and eleven other ministries promulgated the Measures for the Cybersecurity Review, requiring that network products and services involving commercial encryption purchased by critical information infrastructure operators shall undergo the national security review, and the national security shall comply with the requirements of the CSL.

The aforementioned laws, regulations and national standards are not directly related to privacy protection, but the Security Framework for Blockchain stipulates

specific requirements for the privacy protection of the blockchain systems. To be specific:

1) **Principle of Privacy Protection**: The processing of personal information should comply with the principles of lawfulness, legitimacy, necessity and not violate relevant regulatory requirements.

2) **Sensitive Information Protection:** Cryptographic technology should be applied to protect sensitive information, including the content of the transaction and the identity information of the transaction participants. Cryptographic technology should meet the requirements of correctness, anonymity, confidentiality, verifiability and rationality.

3) **Technical Requirements**: The cryptographic algorithms and protocols used need to have provable security. The implementation of privacy protection technology, blockchain applications need to have the ability to improve performance and efficiency or expand functions.

Additionally, the Financial DLT Specification stipulates specific requirements for the management and technologies of privacy protection of the blockchain systems in the financial industry, including:

1) **Strategy of Privacy Protection**: Transaction information and transaction parties' information shall be disclosed, and identity information of transaction parties shall be identified and authenticated. The identity information of transaction parties shall not be fraudulently used, and at least one of the trading content information and trading parties' information shall be encrypted. The participants and auditors shall have the ability to decrypt and verify the encrypted information. The transaction verification node shall be responsible for decrypting and verifying the validity and correctness of encrypted information.

2) **Technical Requirements**: Appropriate technical means should be adopted, in terms of authentication, authorisation, access control, confidentiality, integrity, auditing, monitoring, strategies, etc., to ensure that all stages of the whole lifecycle of private information is not obtained by unauthorised third parties, and to protect the identity of the transaction parties from being identified and fraudulently used.

3) **Monitoring and Auditing**: A complete privacy protection audit plan shall be formulated. The audit contents shall include privacy protection strategies and privacy protection technical means, and the audit forms shall include but not be limited to daily monitoring, regular audit and ad hoc audit.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

There is no law, regulation, regulatory document, nor national standard defining the anonymisation technology. The Institute of Information and Communications Technology, a subsidiary of the MIIT, introduced in Article 4.3 of the Big Data

Security White Paper (2018) that the data anonymisation algorithm may conditionally disclose certain data or certain attribute contents of data, including differential privacy, K-Anonymity, L-Diversity and T-Proximity. The problems to be solved by the anonymisation algorithm include: the balance between privacy and usability, the efficiency of execution, the measurement and evaluation criteria, the anonymisation of dynamically republished data, and the anonymisation of multidimensional constraints. Anonymisation algorithm is widely applied in the field of big data security, because it can prevent sensitive data from being leaked and ensure the authenticity of the published data. The Big Data Security White Paper (2018) is not legally binding.

"Information Security Technology – Guidelines for De-Identifying Personal Information" (the "**Guidelines for De-Identification**") describes pseudonymisation technology in Appendix A "Common De-Identification Technologies" as a de-identification technology that uses pseudonyms to replace direct identifier (or other quasi-identifiers). Pseudonym creation techniques mainly include identifier-independent pseudonym creation techniques and cryptotechnology-based identifier-derived pseudonym creation techniques: (1) identifier-independent pseudonym creation techniques do not rely on the original value of the attribute being replaced, but are generated independently, typically by replacing the original value of the attribute with a random value; (2) cryptotechnology-based identifier-derived pseudonym creation techniques generate pseudonym by using cryptography techniques such as encryption or hashing of attribute values, also known as "key encoding" of attributes in the dataset.

The specific techniques used for anonymisation and pseudonymisation have not been mentioned in the court decisions yet. The introduction of anonymisation and pseudonymisation techniques is not directly related to blockchain techniques and architectures.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

There are several PRC laws and regulations providing general requirements of data localisation and international transfer.

With respect to data localisation, Art. 37 of the CSL stipulates that the critical information infrastructure operators (the "**CIIO**") shall store personal information and important data collected and produced during operations within the territory of China.

In terms of the definition of the critical information infrastructure (the "**CII**"), according to Art. 2 of the Security Protection Regulations on the Critical Information Infrastructure, which was promulgated in July 2021, the CII refers to the important network facilities and information systems in important industries and fields such as public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government and national defense science, technology and industry, as well as other important network facilities and information systems which, in case of destruction, loss of function or leak of data, may result in serious damage to national security, the

national economy and the people's livelihood and public interests. Pursuant to Art. 10 of the CII Regulations and Art. 20 of the Measures for Cybersecurity Review, the identity of the CIIO shall be determined by the PRC government authorities responsible for CII protection, and the identified CIIO shall be notified by the competent PRC government authority.

In addition, there are some industrial rules governing the localised storage of data. For example, in the credit investigation industry, Art. 24 of the Regulation on the Administration of the Credit Investigation Industry stipulates that credit investigation agencies shall sort out, save and process the information they collect within the territory of China. In the taxi online-booking industry, Art. 27 of the Interim Measures for the Administration of Operation and Services of Taxis Subject to Online-booking stipulates that personal information collected and business data generated by taxi online-booking platform companies shall be stored and used in Mainland China. In the healthcare industry, Art. 10 of the Administrative Measures for Population Health Information (Draft) stipulates that population health information shall not be stored in servers in foreign countries, and population health information shall also not be hosted or leased in servers in foreign countries.

With respect to the cross-border transfer of personal information, pursuant to Art. 38–39 and 55 of the PIPL, the cross-border transfers of personal information shall meet any of the following conditions: (1) passing the security assessment organised by the CAC in accordance with Article 40 of PIPL; (2) obtaining personal information protection certification from the relevant specialised institution according to the provisions issued by the CAC; and (3) concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the CAC. Additionally, the personal information processor shall inform the individual of the cross-border transfer, obtain the individual's separate consent and conduct personal information protection impact assessment.

On October 2021, the CAC published the draft Measures for the Security Assessment of Data Cross-border Transfer (the "**Draft Measures for Data Cross-border Transfer**"), which requires that any data processor who provides to an overseas recipient important data collected and generated during operations within the territory of the PRC or personal information subject to security assessment shall conduct security assessment. The Draft Measures for Data Cross-Border Transfer specifies the circumstances in which data processors transfer data across the border shall apply for data cross-border transfer security assessment with the CAC, including, among others, the personal information processors handling the personal information of over one million people providing personal information to overseas parties.

In November 2021, the CAC published the draft Regulations on the Administration of Cyber Data Security ("the **Draft Data Security Regulations**") which also poses other specific requirements in respect of the data cross-border transfer conducted by data processors. Pursuant to the Draft Data Security Regulations, data processors processing personal information of more than one million people shall also comply with the provisions for processing of important data. For example, processors of important data shall specify the responsible person of data safety,

establish a data safety management department and make filing to the cyberspace administration at the districted city level within 15 business days after the identification of their important data.

10. Is it necessary to notify processing activities to any authorities?

The existing laws require the notification of the provision of personal information for the purposes of international judicial assistance or administrative enforcement assistance. In accordance with Art. 36 of the DSL and Art. 41 of the PIPL, where it is necessary to provide personal information outside the territory of China for the purposes of international judicial assistance or administrative enforcement assistance, processors shall apply to the competent authority for approval. CIIO and personal information processors, whose processing of personal information reaches the number specified by the CAC, shall pass the security assessment organised by the authority before providing such information to an overseas party.

Additionally, the Administrative Measures for Data Security (Draft) (the "**Measures for Data Security**") stipulates that a network operator shall file the record of the collection of personal information with the local cyberspace administration authority if it collects personal sensitive information for business operation. The record shall include the rules, purpose, scale, method, scope, type and period of the collection and use, but exclude the content of data. Since the Measures for Data Security have not been officially promulgated, the specific provisions of the Measures for Data Security may be subject to changes.

Moreover, according to the Draft Data Security Regulations, data processors shall apply for the cybersecurity review when carrying out the following activities: (a) the merger, reorganisation or separation of internet platform operators that have acquired a large number of data resources related to national security, economic development or public interests, which affects or could affect national security; (b) data processors that process the personal information of more than one million people intend to be listed overseas; (c) data processors intend to be listed in Hong Kong, which affects or may affect national security; and (d) other data processing activities that affect or may affect national security.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

Art. 44–50 of the PIPL, Art. 43 and 49 of the CSL, Art. 9 and 11 of the Provisions on the Protecting the Personal Information of Telecommunication and Internet Users, Art. 6 of the "Guidelines for Self-Assessment of Collecting and Using Personal Information by Mobile Internet Applications (App)", Art. 6 of the "Methods for Identifying the Illegal Collection and Use of Personal Information by Apps" and Art. 8 of the PIS Specification, specify the rights of an individual as follows:

1) **Right to be Informed, Make Decisions and Require an Explanation**: An individual shall be entitled to know and make decisions on the processing of his/her personal information, and to restrict or refuse the processing of his/her personal information by others, unless otherwise prescribed by laws and administrative regulations. An individual shall also be entitled to require

a personal information processor to explain its rules on personal information processing.

2) **Right to Access and Duplication**: An individual shall be entitled to access or copy his/her personal information from personal information processors, except under the circumstances specified in the PIPL. Where an individual requests to access or copy his/her personal information, a personal information processor shall make available the personal information in a timely manner.

3) **Right to Make Corrections or Supplements**: An individual who finds that his/her personal information is inaccurate or incomplete shall be entitled to request the relevant personal information processor to correct or supplement the personal information. Where an individual requests for correction or supplementation of his/her personal information, the relevant personal information processor shall verify his/her personal information and make correction or supplementation in a timely manner.

4) **Right to Deletion**: Under any of the following circumstances, a personal information processor shall delete an individual's personal information on its own accord; where the personal information processor fails to do so, the individuals shall have the right to request the processor to delete: (a) Where the purposes of personal information processing have been achieved, or can not be achieved, or the data is no longer necessary for achieving that purpose; (b) Where the personal information processor stops providing products or services or the retention period has expired; (c) Where the individual withdraws consent; (d) Where the personal information processor processes personal information in violation of laws, administrative regulations or agreements; or (e) Where there are any other circumstances stipulated by laws and administrative regulations.

5) **Right to Withdrawal of Consent**: An individual shall be provided with the method to withdraw their consent to collection and use of their personal information. The personal information subjects shall have the right to refuse to receive commercial advertisements pushed depending on their personal information.

6) **Right to Cancel the Account**: The personal information processor shall provide the personal information subject with a convenient and easy-to-operate method for account cancellation. If manual handling is required after the request for account cancellation is received, the verification and handling shall be completed within the promised time limit.

7) **Right to a Passed Individual**: In the event that an individual passed away, his/her close relatives may exercise the rights of access, duplication, correction and deletion in relation to the relevant personal information of the deceased for their own interests, unless the deceased has made other arrangements when he/she was alive.

8) **Right to Report and Complaint**: A personal information processor shall establish a convenient mechanism to accept and process applications by

individuals for exercising their rights, and shall explain reasons if it rejects an individual's request to exercise rights. Where a personal information processor refuses an individual's request to exercise rights, the individual may file a lawsuit with the competent court.

9) **Right to Portability**: Where the request of an individual for transferring personal information to his/her designated personal information processor satisfies the conditions prescribed by the CAC, the relevant personal information processor shall provide the channels for such transfer.

The right to be forgotten does not exist in China. The difference between the right to deletion and the right to be forgotten is that the right of deletion can only be exercised under limited conditions. Only when the data controller violates laws, regulations or agreements, can the personal information subject request deletion. In contrast, the right to be forgotten can be exercised, when the purpose of collecting data no longer exists, or when a personal information subject withdraws his consent. In addition, Chinese courts have denied the right to be forgotten in judgments. In the case of Ren Jiayu v. Baidu (the dispute over the right to reputation in 2015), Beijing No. 1 Intermediate People's Court decided that "the right to be forgotten" is not stipulated under the current Chinese laws, and there is no legitimate and necessary personal interest in protecting "right to be forgotten".

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

The Financial DLT Specification divides financial blockchain service providers into financial distributed ledger operators and financial distributed ledger system builders, and the CSL distinguishes network operators from other technical service providers. The Financial DLT Specification can apply to public blockchain in the financial sector, and the CSL can apply to public blockchain in the non-financial sector. To be specific:

1) **Network Operators/Financial Distributed Ledger Operators:** According to Art. 14 of Financial DLT Specification, financial distributed ledger operators collect, transmit, store, present, inform, de-register and process the account information, identification information, transaction information, personal identity information, property information and other information reflecting the activities of specific natural persons. Network operators or financial distributed ledger operators will participate in the processing of personal information.

2) **Technical Service Providers/Financial Distributed Ledger System Builders:** After technical service providers (which are known as financial distributed ledger system builders in the financial industry) establish the blockchain system, they deliver the blockchain system to the service operator, and they do not directly participate in personal information processing activities, so there is no need for technical service providers to perform the obligations of personal information protection.

The Security Framework for Blockchain further expands the actors in the blockchain. To be specific:

1) **Blockchain End Users:** A blockchain end user refers to any organisation or individual who uses the blockchain.

2) **Blockchain Business Providers:** A blockchain service provider refers to the entity that provides blockchain services, which is responsible for developing business programs, deploying, operating, managing and maintaining blockchain networks and nodes, and directly or indirectly providing services to blockchain end users.

3) **Blockchain Technology Providers:** A blockchain technology provider refers to an institution or organisation that provides technical support for blockchain business providers, and is responsible for developing blockchain and its applications, creating and maintaining codes and special equipment, and providing related technical support and services.

4) **Blockchain Auditors:** A blockchain auditor is responsible for performing audits in the supply and use of blockchain businesses. Blockchain audits typically cover operations, performance, and security, primarily to check whether relevant auditing criteria are being met. Auditors need to follow the principles of independence and objectivity, use systematic and standardised methods, and promote business and technology providers to establish and continuously improve effective risk management, internal control compliance, and governance structures through supervision, evaluation, and consultation in order to achieve blockchain business goals.

5) **Blockchain Regulators:** A blockchain regulator supervises and inspects the blockchain in accordance with relevant policies and regulations, maintains the legal, safe and stable operation of the blockchain, and cooperates with blockchain technology providers to provide regulatory technology and interfaces.

In addition, data processing agencies in the field of blockchain can be divided into personal information controllers (or personal information processors) and entrusted processors (or entrusted parties). Personal information controllers, who are capable of determining the purposes and methods of personal information processing, directly enter into service agreements with clients of the blockchain system, and directly assume the obligations of personal information protection. The personal information controller delegates the processing of personal information in a blockchain system to entrusted processors, the personal information controller requires the entrusted processor to satisfy the corresponding technical and management requirements under the entrustment contract.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

There are only a few laws, regulations and national standards on blockchain in the PRC. Among all the laws, regulations and national standards on blockchain, only

the Financial DLT Specification and the Security Framework for Blockchain have the provisions of privacy protection.

Even though there is no specific law or regulation on the personal information protection in the field of blockchain, the blockchain is "the system that is composed of computers or other information terminals and relevant equipment and collects, stores, transmits, exchanges, and processes information in accordance with certain rules and procedures", and this is the concept of network as set forth in the CSL. Since the blockchain is a network, the provisions of personal information protection in the CSL and supporting documents of the CSL can apply to blockchain.

In addition, blockchain service providers (especially identity registration institutions) collect and use personal information, so the laws or rules on the personal information protection in data processing activities, such as the PIPL and the PIS Specifications, are applicable to blockchain service providers.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

When using public blockchains and private blockchains to store, use, and transfer personal information and other data, it should comply with the requirements of the PIPL and the DSL and other relevant regulatory requirements. To be specific:

1) **Rights of Individuals:** Data can only be added on blockchains through consensus algorithms, and cannot be modified or deleted to prevent tampering. To a certain extent, blockchain technology conflicts with the rights of deletion and correction of personal information, which stems from the distribution of blockchains.

2) **Content Governance:** Due to the immutability of public blockchains, it is difficult to effectively process, block or delete on-chain data. According to Provisions on the Governance of the Online Information Content Ecosystem promulgated in March 2020, online information content shall not harm national interests, public interests and the legitimate rights and interests of others. Therefore, measures shall be taken to prevent and resist the production, reproduction, and publication of illegal and bad information.

3) **Cross-border Transfer:** Blockchain technology transcends national borders, so end users of the blockchains come from all over the world. This may be identified as cross-border transfer by the CSL and the PIPL, while the PRC laws and regulations impose many restrictions and compliance requirements on cross-border transfer.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

Public blockchains rely on nodes to verify and process transactions or execute smart contracts in a global open network. On a public blockchain, anyone can run a node and start validating transactions or ensuring smart contracts are executed

according to cryptographic rules, and each node keeps an updated version of the state as long as it is corrected to the network. The data stored on public blockchains is completely tamper-proof and immutable.

Private blockchains are distributed ledger technology consisting of many databases and operated by a limited set of companies. On a private blockchain, permission is essential for the access to the network, and consensus on the latest state of the database is enforced by a small number of trusted parties. Other parties in the network can read the database but cannot change it.

According to the Blockchain White Paper (2020) issued by the China Academy of Information and Communications Technology, privacy issues in the process of data circulation have become increasingly prominent. Information on the blockchains, such as user identity information, asset information, transaction flow and other information requires certain technical means to improve the privacy protection capability in the process of data circulation.

According to the industry practice, the commonly used practices for processing personal information on both public and private blockchains include:

1) **Choosing a blockchain deployment method with less compliance risk:** Since the private blockchain limits the open scale and entities of nodes, compared with the public blockchain that anyone can participate in, the data on the private blockchain can be processed within a controllable range. If the blockchains have the licensing mechanism to verify and register nodes, personal information can be more effectively protected.

2) **Setting up a manual intervention mechanism**: In order to protect personal information, appropriate human intervention mechanisms need to be set up on the blockchains. For example, if the on-chain information cannot be directly corrected or deleted after being time stamped, it is necessary to rewrite the information by adding code to ensure accuracy. Manual review and correction mechanisms should also be implemented in automated decision-making.

3) **Adopting appropriate technical and organisational measures:** After the information is encrypted by asymmetric encryption and anonymisation technology, organisational measures such as restricting access control and storing information separately should be taken, so that the information will not be used to re-identify an individual. In addition to common technical measures (such as data encryption and permission control), cut-of-edge technical means, such as zero-knowledge proof, homomorphic encryption, TEE, MPC, federated learning, are applied to improve the privacy protection capability in multi-party collaborative scenarios, which makes the data on blockchains "available but invisible".

4) **Distinguishing the roles and responsibilities of parties in the blockchain:** There are multiple actors in the blockchain, such as blockchain end users, blockchain service providers, blockchain technology providers, blockchain auditors and blockchain regulators, etc. Since a series of obligations and responsibilities under the PIPL are carried out around the personal

information processors, it is essential to identify whether actors are the personal information processors.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

The "travel rule" requires VASPs, including virtual asset exchanges, to obtain and save relevant information when a client deposits assets to an exchange. It also requires VASPs to obtain and save recipient account information, when a clients' assets are sent to another account. Whenever a virtual asset transaction is made, this information must also be transmitted to the asset recipient. While the FATF's Guidelines are not legally binding, countries that choose not to comply could risk being punitively excluded from the global financial network. At present, Chinese laws and regulations have not localised FATF's travel rules.

According to FATF, "A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations"[54]. At the same time, Gou Wenjun, Secretary of the Party Committee and Director of the China Anti-Money Laundering Monitoring and Analysis Center of the Central Bank, said that from the general consensus of relevant international financial organisations, financial departments, and the Central Bank, "virtual assets" exclude fiat currencies and financial products with a real basis. Therefore, virtual assets do not include digital currency,

From the perspective of virtual currency transactions, since China has begun to take measures to prohibit virtual currency transactions, travel rules are meaningless in China. To be specific:

1) In September 2021, the Notice on Further Preventing and Dealing with Speculation Risks in Virtual Currency Trading (the "**NPVC**") was issued, which states that virtual currencies do not have the same legal status as legal tender, and the business activities related to virtual currencies are illegal financial activities.

2) In September 2021, the CAC, the MPS and other competent departments jointly issued the Notice on Renovating Virtual Currency "Mining" Activities (the "**NVCM**"), which forbids carrying out virtual currency "mining" activities in the name of a data centre. New additional physical mining projects are strictly prohibited, and existing projects will also be withdrawn under the NVCM.

54 https://www.fatf-gafi.org/glossary/u-z/#:~:text=A%20virtual%20asset%20is%20a%20digital%20representation%20of,are%20already%20covered%20elsewhere%20in%20the%20FATF%20Recommendations.

Hong-Kong

Authors

Gabriela Kennedy, Mayer Brown

Karen H. F. Lee, Mayer Brown

Cheng Hau Yeo, Mayer Brown

1. What are the legal acts regulating data privacy in your jurisdiction?

The Personal Data (Privacy) Ordinance (Cap 486) ("**PDPO**") is the principal legislation that regulates the collection, use, transfer, processing and storage of personal data by an entity (i.e., a data user) in Hong Kong. In general, the PDPO requires all organisations that control the collection, use and processing of personal data for their own purposes to comply with six data protection principles which articulate the main requirements regarding the privacy of personal data, namely the purpose and manner of collection, accuracy and duration of retention, use of personal data, data security, openness and transparency, and access and correction.

In addition, the Personal Data (Privacy) (Amendment) Bill 2021 which was recently passed on 29 September 2021 aims to combat doxxing in Hong Kong by introducing new doxxing-related offences and enhancing the powers of the Office of the Privacy Commissioner for Personal Data ("**PCPD**") to tackle doxxing incidents.

Separately, there are also other proposals being put forward to amend the PDPO. The key proposals are: (1) the introduction of a mandatory data breach notification regime; (2) the requirement for data users to put in place data retention policies; (3) the direct regulation of data processors; (4) expanding the definition of "personal data"; and (5) a review of the penalties that may be imposed for a breach of the PDPO. These amendments are likely to be introduced in 2022.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

The Office of the PCPD is the main body responsible for overseeing the enforcement of the PDPO and is headed by the PCPD.

The PCPD has various investigative powers, including the right to:

- undertake investigations and inquiries and issue enforcement notices in the event of any breach of the PDPO;
- enter any premises for investigation or inspection purposes (subject to certain requirements);

- conduct inspections on any personal data system (i.e., a system, whether or not automated, used in whole or in part, by a data user to collect, hold, process or use personal data); and

- summon and examine the claimant or any person who the Privacy Commissioner believes has information regarding an investigation and require such persons to provide any information relevant to an investigation the PDPO is conducting.

In addition, pursuant to the Personal Data (Privacy) (Amendment) Bill 2021, the PCPD has additional powers to conduct criminal investigations and institute prosecution for doxxing cases. The PCPD also has the power to issue cessation notices to Hong Kong persons or non-Hong Kong service providers to demand certain actions to be taken, which include:

- removing doxxing messages from electronic platforms;

- prohibiting or limiting access to the doxxing message or the relevant platform on which the doxxing message is published; and

- discontinuing hosting services for part of or the entire platform on which the doxxing message is published.

Any breaches of the PDPO that amount to an offence, or any breach of an enforcement notice issued by the PCPD, are referred to the police for possible prosecution.

In addition, to the extent that any data privacy or blockchain issues may arise in relation to any financial institutions or entities authorised to deal with structured products, the Hong Kong Monetary Authority ("**HKMA**") and the Securities and Futures Commission ("**SFC**") may also have jurisdiction.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

No specific regulations or guidelines on blockchain have been published by the PCPD so far. However, the PCPD published an article on blockchain and data protection in the Hong Kong Lawyer journal in July 2019. The article provides an explanation of the key concepts of blockchain and discusses the privacy issues that may arise from the application of blockchain for various purposes. In particular, the article highlights three main privacy risks:

- Transaction data (which may contain personal data) stored on the blockchain distributed ledger system may be openly displayed to all participants of the blockchain, including future new participants who may join the network from time to time. This may conflict with the basic data protection principle that data subjects should be notified of the identity of the data user who collects their personal data and the class of persons to whom such data will potentially be disclosed. The privacy risk in this regard is more significant for “permissionless” or public blockchains (where any person is allowed to join and access the transaction data without prior approval required) as compared to private blockchain networks.

- The blockchain network is known for its immutability, which means the transaction records are tamper-proof once they are recorded to the open and distributed ledger, and no deletion or correction to such records will be possible even if the data contained in those records are obsolete or inaccurate. Therefore, these features of blockchain appear to be incompatible with a data subject's general right to data accuracy and erasure.

- Given the distributed nature of blockchain technology, the responsibility for the administration of a blockchain does not fall on a single entity. Therefore, the lack of a clear data user results in certain issues such as difficulties faced by regulators in enforcing data privacy regulations and difficulties faced by data subjects in asserting their data privacy rights (e.g., submitting a data access request).

The article also refers to the guidance on the use of blockchain provided by the Commission Nationale de l'Informatique et des Libertés ("**CNIL**"), the data protection authority in France, where the regulator suggests that organisations should think twice before embarking on adopting blockchain technology and prioritise data minimisation in view of the shared nature. Also, as a blockchain has a decentralised system, it is recommended that participants be regarded as data users to ensure accountability.

It is also important to note that, according to the article, the PCPD expects organisations to adhere to the principles of accountability and ethics when using blockchain technology. In particular, the PCPD requires privacy impact assessments and ethical data impact assessments to be carried out prior to the use of blockchain.

Following the 2019 article, the PCPD published another article on the "Application of Blockchain" in the Hong Kong Lawyer journal in March 2020. The articles discusses the various applications of blockchain apart from being used in relation to digital currencies or FinTech – these applications include dispute resolution, motor insurance and cross-border money transfers. The article also reiterates the point that there are currently no specific regulations on blockchain in Hong Kong, although the SFC has set out its regulatory approach for virtual asset trading platforms in November 2019. For example, platforms that offer the trading of security tokens can apply to be licensed under the regulatory regime, provided that these operators are able to meet robust regulatory standards that address risks associated with virtual assets. In addition, licensed platforms will be placed in a "regulatory sandbox" for a period of intensive supervision. The article also made comparisons to Mainland China where several regulations relating to blockchain have been released.

Separately, the HKMA has issued two whitepapers on the topic of distributed ledger technology. The most recent was issued in October 2017 (Whitepaper 2.0 on Distributed Ledger Technology). Under the Whitepaper 2.0, the HKMA identified a number of potential legal issues concerning data privacy. These largely reflect the same concerns raised by the PCPD, discussed above. It also highlighted issues regarding the cross-border nature of blockchain technology, such as the

difficulty in identifying governing laws, and any cross-border transfer or data localisation restrictions.

4. What kind of actors (e.g., data subjects, controllers, processors...) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

There are three types of actors defined in the PDPO: data subjects, data processors and data users. Under the PDPO:

- a "data subject" is defined as "in relation to the personal data, the individual who is the subject of the data";
- a "data user" is synonymous as a data controller under section 2(1) of the PDPO, and is defined as "in relation to the personal data, a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data"; and
- a "data processor" is defined under Data Protection Principle 2(4) as "a person who: (i) processes personal data on behalf of another person; and (ii) does not process the data for any of the person's own purposes.

Data processors are not directly regulated by the PDPO. The data user will be ultimately accountable in the event of any breach of the PDPO caused by its data processors. Further, where a data user engages a data processor to process personal data on the data user's behalf, the PDPO requires the data user to adopt contractual or other means to prevent any personal data from being kept longer than necessary for processing of the data, and to prevent unauthorised or accidental access, processing, erasure, loss or use of personal data that has been transferred to the data processor for processing.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Under section 2(1) the PDPO, personal data refers to "any data: (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable".

The PDPO does not provide for different categories of personal data (e.g., sensitive vs. non-sensitive data). However, the PCPD has published certain guidelines, such as the Guidance on Collection and Use of Biometric Data (August 2020) and the Code of Practice on Consumer Credit Data (Revised in 2013), regarding the collection and use of certain types of personal data that he considers to be particularly sensitive, and which need to be approached with caution. These include Hong Kong Identity Cards ("**HKID**"), consumer credit data and biometric data. In particular, unless required by law, data users must not make it mandatory for an individual to provide their HKID card number or a copy of their HKID card.

In general, personal data that may be seen as particularly sensitive (e.g., medical records, financial information, biometric data, HKID numbers, etc.) should not be collected (even if provided on a voluntary basis), unless it is required by law or it is

absolutely necessary in order for the data user to carry out the purpose of collection (e.g., there is no other less privacy intrusive method available, and such data is needed to provide the services to the data subject).

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

The PDPO does not provide definitions of "anonymisation" and "pseudonymisation".

However, the PCPD has published the Guidance on Personal Data Erasure and Anonymisation ("**Guidance on Anonymisation**") which states that anonymising personal data means "removing from the personal data any information from which an individual may be identified by anyone reading the record" such that "the data user is not in a position to re-establish the identity of any individual with its other existing or future information on the individual".

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

There is currently no legislation in Hong Kong that specifically regulates the use of blockchain technology.

However, as mentioned above, it should be noted that the Hong Kong Securities and Futures Commission ("**SFC**") issued a position paper in November 2019 which sets out a new regulatory framework for crypto exchanges and virtual asset trading platforms. For example, licences may be granted to platforms that offer trading of security tokens provided that the operators have the ability to meet robust regulatory requirements that deal with virtual assets. Those who are licensed will be placed in a "regulatory sandbox" and subject to closer monitoring and supervision by the SFC. Following the publication of the position paper, in December 2020 the SFC announced that it has granted the first licence to a virtual asset trading platform in Hong Kong.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

Under the Guidance on Anonymisation, the PCPD provides guidelines on the use of anonymisation techniques as an alternative to the erasure of personal data which is no longer required for the purpose for which it was used. Where personal data is anonymised such that no specific individual can be directly or indirectly identified from the data, such data will no longer be considered personal data under the PDPO and the data user may continue to retain such data for other purposes (e.g., research and statistical purposes). However, the Guidance on Anonymisation does not make any specific reference to any blockchain-based applications and architectures.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

Under the PDPO there are no specific restrictions currently in force in respect of data localisation or the transfer of personal data outside of Hong Kong.

Section 33 of the PDPO, which imposes restrictions on the transfer of personal data outside of Hong Kong, has been on the statute books since the PDPO was enacted in 1996. However, Section 33 has yet to come into force. When it does come into operation, Section 33 of the PDPO shall prohibit the transfer of personal data from Hong Kong to another jurisdiction, except in one or more specified circumstances.

Even though Section 33 is not yet in operation, data users may only transfer personal data to a third party (whether inside or outside Hong Kong) if:

- it is to a recipient that falls within one of the categories of transferees notified to the data subject on or before the collection of his or her personal data (this is part of the notification requirements that must be fulfilled before a data subject's personal data may be collected);
- the transfer is pursuant to the consent provided by the data subject; or
- one of the exemptions to consent specified under the PDPO applies.

10. Is it necessary to notify processing activities to any authorities?

It is not necessary for an entity to notify any Hong Kong authorities of its processing activities.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

- Right to access and correct data

  Under the PDPO, a data subject has the right to ascertain whether a data user holds personal data of which he or she is the data subject and to request a copy of such data. In addition, a data subject also has the right to request the correction of his or her personal data.

- Right to be forgotten

  The PDPO does not expressly provide for a "right to be forgotten". However, there is a general requirement under the PDPO for a data user to take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was originally collected, unless such erasure is prohibited under any law or it is in the public interest (including historical interest) for the data not to be erased.

  In addition, certain rights to erasure are provided to individuals in relation to the banking sector. Under the code of practice on consumer credit data

published by the PCPD, credit providers are required to notify data subjects of their right to instruct the credit providers to request a credit reference agency to delete their account data in relation to a terminated account.

Under the Code of Banking Practice published by the Hong Kong Association of Banks, banking institutions are also required to implement the appropriate measures to acknowledge the rights of consumers to require the prompt correction and/or erasure of inaccurate, or unlawfully collected or processed data.

- Objection to and opt out of direct marketing

  A data subject may at any time request that the data user cease using or cease disclosing their personal data for direct marketing purposes. The data user must comply with the data subject's request to unsubscribe from receiving any further direct marketing materials, at no charge, even if the personal data was not collected by the data user directly from the data subject. The data subject can communicate their request in any manner whatsoever, i.e., orally or in writing.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

As a public (i.e., permission-less) blockchain network typically allows any member of the public to transact, participate, and gain access to all information in the network apart from the private keys, each network participant could potentially be considered as a data user under the PDPO (to the extent that the blockchain contains personal data) since he or she is able to "control the collection, holding, processing or use" of such publicly accessible data, and would therefore be subject to all relevant obligations of a data user under the PDPO.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The PDPO may potentially apply to private and permissioned blockchains to the extent that they contain personal data. This is because the PDPO regulates the handling and processing of all personal data.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

As there are no specific regulations relating to blockchain, the general requirements regarding the use, transfer and storage of personal data under the PDPO would apply (to the extent that the blockchain contains personal data).

- Limits on use of personal data

  Yes. A data user may collect personal data from data subjects only if:

- the personal data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the personal data;
- the collection of personal data is necessary for and directly related to that purpose; and
- the personal data is adequate, but not excessive in relation to that purpose.

When collecting personal data directly from a data subject, the data user is also subject to certain notification requirements, unless an exemption applies.

Additionally, consent is required if the personal data will be used or transferred for direct marketing purposes, or for any other purpose that is not covered by the original collection purpose (as notified to the individual at the time of collection) or a directly related purpose, unless an exemption applies.

- Limits on transfer of personal data

  A data user can only transfer personal data to a third party (whether inside or outside Hong Kong) if it is to a recipient that falls within one of the categories of transferees notified to the data subject on or before the time the data was collected. Otherwise, the consent of the data subject is required unless an exemption applies.

  In addition, when transferring personal data to a data processor, the data user must adopt contractual or other means to prevent:

  - personal data that is transferred to the data processor from being kept for longer than is necessary for the processing of such personal data; and
  - any unauthorised or accidental access, processing, deletion, loss or use of the personal data that is transferred to the data processor.

- Limits on storage of personal data

  Under the PDPO, data users must take all practicable steps to ensure that personal data is not held longer than is necessary to fulfil the purpose (or a directly related purpose) for which the personal data was collected for, and is erased when no longer required for such purposes, unless any such erasure of the personal data is prohibited by law or the retention of the data is in the public interest (for instance, historical interest). Additionally, as mentioned above, where data users engage data processors, they must adopt contractual or other means to prevent their data processors from keeping personal data longer than is necessary for processing the data.

  While the PDPO does not stipulate any retention periods for personal data, data users should refer to the requirements under other statutes and various guidelines issued by the PCPD and other industry-specific

regulators. For instance, the PCPD's Code of Practice on Human Resource Management provides that employers may retain the personal data of an employee for up to seven years after the end of the employee's employment, unless there is a subsisting reason that requires the employer to hold the data for a longer period, or the data is necessary for the employer to comply with contractual or legal obligations.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

As mentioned in the Hong Kong Lawyer journal article published by the PCPD in March 2020, apart from digital currencies and FinTech applications, common use-cases for public and private blockchains in Hong Kong include dispute resolution processes, motor insurance and cross-border money transfers. While there are no regulations that specifically regulate the use of blockchain, the relevant stakeholders will have to ensure that such applications of blockchain technology are compliant with the requirements of the PDPO (to the extent that personal data is involved), and practices have to be formulated and designed in a manner that ensures such data privacy compliance.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

According to an executive summary published by the FATF in 2019 which evaluated the level of compliance with the FATF 40 Recommendations in Hong Kong, Hong Kong has a "reasonably good" level of understanding of money laundering risks, although their verdict is more reserved with regard to higher risks areas such as money laundering linked to foreign tax and corruption offences. Hong Kong has also been viewed as being competent in confiscating illegal proceeds and prosecuting money laundering offences with a high conviction rate, although the sentences imposed are at the lower end compared to other major jurisdictions.

In relation to Recommendation 16 (the Travel Rule), the Hong Kong Financial Services and the Treasury Bureau ("**FSTB**") has recently concluded a consultation paper which proposes to introduce a new regulatory regime which will result in all virtual asset platforms operating in the region being regulated by the SFC, including those with virtual assets that do not qualify as "securities". In particular, Hong Kong's AML legislation will be extended to cover all virtual asset platform providers, under which these providers must provide the following information to the HKMA for funds transfer transactions above HK$8,000:

A. Originator's and beneficiary's names

B. Numbers of originator's and beneficiary's account maintained with their relevant institutions in relation to the wire transfer, or, in the absence of such numbers, the relevant unique reference numbers

C. The originator's address, customer identification number, identification document number, or place and date of birth (for natural persons).

According to the FSTB, they are targeting to introduce the amendment bill into the Legislative Council in the 2021–22 legislative session.

India

Authors

Anirudh Rastogi, Ikigai law

Sreenidhi Srinivasan, Ikigai law

Mayank Takawane, Ikigai law

1. What are the legal acts regulating data privacy in your jurisdiction?

Presently, there is no comprehensive law dealing with data privacy in India. The Indian data protection and privacy framework is embodied in India's Information Technology Act, 2000 (**IT Act**)[55], and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**SPDI Rules**)[56].

However, a dedicated personal data protection law is currently under development – this is the Personal Data Protection Bill, 2019 (**PDP Bill**)[57] which borrows, to a limited extent, from the European Union's General Data Protection Regulation (**GDPR**). The PDP Bill is currently being examined by a Joint Parliamentary Committee[58] gathering members from both houses of the Indian Parliament. The Committee adopted its report on 22 November 2021 and will table its recommendations before the Indian Parliament.

The Ministry of Electronics and Information Technology (**MeitY**) instituted a Committee of Experts in September 2019 to recommend a framework to govern non personal data[59]. The Committee of Experts on Non-Personal Data Governance Framework (**NPD Committee**) released a draft report on 12 July 2020[60], and a revised version of its report on 16 December 2020[61]. The final report is yet to be made public. The relevant portions of the revised report are discussed in this section.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

Currently, there is no exclusive authority to enforce data protection laws in India. However, the PDP Bill envisages the establishment of a Data Protection Authority

[55] See https://www.indiacode.nic.in/handle/123456789/1999.

[56] See https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_15178073240777&type=rule&filename = GSR313E_10511(1)_0.pdf.

[57] See http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[58] See http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1.

[59] See https://meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_ framework.pdf.

[60] See Report by the Committee of Experts on Non-Personal Data Governance Framework, https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-datagovernance-framework.pdf.

[61] Ibid., p. 41.

of India (**DPAI**) (Clause 41). The proposed DPAI will be responsible for protecting the interests of data subjects, preventing any misuse of personal data, ensuring compliance with the provisions of the Act, and promoting awareness about data protection.

The NPD Committee's report recommends the establishment of a Non-Personal Data Authority (**NPDA**). However, reportedly, the next version of the PDP Bill will suggest that non-personal data should also be governed by the DPAI set up under the PDP Bill framework.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

Currently there is no exclusive authority to enforce data protection laws in India, and therefore there are no corresponding regulations/guidance/opinions applicable to blockchain technology.

However, some other ministries and regulators have released guidance/opinions relevant to blockchain technology. Key takeaways include:

1) The Reserve Bank of India (**RBI**) (India's central bank):

   a) In January 2017, the Institute for Development and Research in Banking Technology (**IDRBT**), which was established by the RBI in 1996 to study the intersection of banking and technology, released a white paper entitled "White Paper: Applications of Blockchain Technology to Banking and Financial Sector in India",[62] which noted:

      i) Banks should run internal experiments and pilot projects first and then move to interbank applications such as centralised "Know Your Customer", cross-border payments, syndication of loans, trade finance, capital markets, supply chain finance, bill discounting, monitoring of consortium accounts and servicing of securities to facilitate use of blockchain technology.

      ii) Blockchain technology has matured enough and there is sufficient awareness among the stakeholders which makes this an appropriate time for initiating suitable efforts towards digitising the Indian Rupee through blockchain.

      iii) There are cost-saving, transparency, and efficiency advantages of the technology and the time is ripe for its adoption in India.

   b) In January 2019, The IDRBT released a "Blueprint of Blockchain Platform for Banking Sector and beyond",[63] which noted:

      i) Blockchain can address some of the gaps in current systems. It is necessary to set up a blockchain network involving a large number of businesses to participate and simplify communication related to their transactions.

[62] See IDBRT whitepaper, available at https://idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf.
[63] Ibid., p. 26.

ii) A common standardised infrastructure must be set up to facilitate business development of communication networks.

iii) A governance structure besides the layers of applications and services, headed by a steering committee to oversee the implementation of a platform based on blockchain technology is suggested.

iv) There is a need to create an industry-specific business value framework for analysing suitability of business applications to be migrated to blockchain based business networks.

c) IDRBT is engaged in a research project entitled "Distributed Center of Excellence for Blockchain Technology"[64], sponsored by MeitY. Key objectives of the project include:

i) Evolving a blockchain ecosystem around R&D organisations, government departments and academia.

ii) Conducting research on issues and challenges related to blockchain usage in identified application domains and enhancing capacity-building in blockchain technology.

iii) The report with the findings of the research project is yet to be released publicly, though in its National Strategy on Blockchain (discussed in 4(b) below), the MeitY notes that certain agencies, including the IDBRT have carried out research on the use of blockchain technology in identified domains and have developed proof-of-concept solutions and piloted them.

d) On 11 February 2020, the RBI released a notification, "Distributed Ledger Technology, Blockchain and Central Banks",[65] which noted:

i) Distributed ledger technology (**DLT**) and blockchain technology have the potential to provide solutions to the financial sector.

ii) Increasing support from RBI and government of India through regulatory sandbox and other mechanisms will help support innovation in blockchain.

iii) Blockchain technology has characteristic features such as hash function, nodes, blocks and tokens.

iv) Various developments have taken place with regard to adopting DLT and blockchain by start-ups and financial institutions[66].

[64] Ibid., p. 26
[65] See https://m.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=18766.
[66] See Table 2 of the notification, available at https://m.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=18766.

2) Securities and Exchange Board of India (**SEBI**):

a) In August 2017, a Committee on Financial and Regulatory Technologies (**CFRT**) was set up to explore the possibility of implementing blockchain in stock markets[67]. The CFRT is yet to release its report. The terms of reference of the CFRT specifically envisage exploring DLT technologies[68].

b) In August 2021, a circular titled "Securities and Covenant Monitoring using Distributed Ledger Technology" was issued by SEBI, which noted:

i) A system using Distributed Ledger Technology (DLT) shall be used from April 01, 2022: (1) for recording of and monitoring of securities by the issuer of the securities; (2) for continuous monitoring of covenants by debenture trustees; and (3) for credit rating of the non-convertible securities by the credit rating agencies, etc.

ii) DLT has the potential to provide a more resilient system than traditional centralised databases and offer better protection against different types of cyber-attacks because of its distributed nature, which removes the single point of attack.

iii) Depositories are advised to formulate operational guidelines after consulting with various stakeholders.

c) In October 2021, SEBI advised Investment Advisors to refrain from engaging in unregulated activities, such as providing platform for buying/selling/dealing in unregulated products.[16] While the press release made a reference to digital gold, it did not make any reference to cryptocurrencies or crypto assets. However, given that they are unregulated products in India, the press release has been interpreted as refraining Investment Advisors from providing crypto related advice.

3) NITI Aayog:

a) In January 2020, "Draft Discussion Blockchain: The India Strategy",[69] was released by NITI Aayog, which noted:

i) Regulatory and policy considerations must be developed for evolving a vibrant blockchain ecosystem.

ii) Creation of a national infrastructure for deployment of blockchain solutions with inbuilt fabric, identity platform and incentive platform is recommended.

---

[67] See https://www.sebi.gov.in/media/press-releases/aug-2017/sebi-constitutes-committee-on-financial-and-regulatorytechnologies-cfrt-_35526.html.

[68] See https://www.tokenpost.com/Indian-regulators-want-to-explore-blockchain-for-securities-market-4915.

[69] See NITI Aayog's Blockchain India Strategy Part I, available at https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf.

iii) Promotion of research and development in blockchain, in addition to a focus on skilling the workforce and students to develop India as a blockchain hub should be pursued.

iv) A stablecoin pegged to the Indian Rupee for seamless exchange on blockchain solutions must be introduced. This may require a re-evaluation of India's stance on cryptocurrencies.[70]

4) MeitY:

a) In 2019, MeitY released "India's Trillion-Dollar Digital Opportunity"[71] which noted:

i) Blockchain creates an efficient and cost-effective database that is virtually tamperproof. Blockchain can play an important role in storing individuals' data, helping conduct secure transactions, and maintaining a permanent and private identity record.[72]

ii) The private sector in India has started working on blockchain applications such as ICICI Bank, Mahindra, IBM and Bajaj Electricals.

b) In February 2021, the MeitY released a draft "National Strategy on Blockchain",[21] which:

i) Suggested the creation of a "National Level Blockchain Framework" to host sector specific blockchains (such as blockchain for health, insurance, and education).[22]

ii) Highlighted scalability, security and lack of awareness as some of the technical challenges, in adopting blockchain technology, and data regulations, banking regulations, and the IT Act as some of the legal challenges faced.[23]

iii) Set out a roadmap to boost the adoption of blockchain, particularly in the public sector.[24]

5) Others:

a) Department of Economic Affairs, Ministry of Finance: In 2019, the department released a "Report of the Steering Committee on FinTech Related Issues" which noted:

i) Blockchain can be deployed for use in major fintech applications such as cross-border payments, settlement of securities, trade finance and smart contracts.

[70] Ibid., p. 52.

[71] See https://www.idrbt.ac.in/externalprojects.html#:~:text=The%20Institute%20has%20been%20awarded,MeitY)%2C%20Government%20of%20India.

[72] See https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf.

b) Competition Commission of India (CCI): In April 2021, the CCI released a "Discussion paper on Blockchain and competition",[25] which:

   i) Highlighted potential antitrust issues that arise in functioning of blockchain systems, including abuse of dominance, and anti-competitive agreements.

   ii) Suggested that blockchain may be similar to partnerships or multi-party contracts, without considering it as a unique phenomenon that needs its own novel legal understanding.[26]

   iii) Suggested that Blockchains may not be fully compatible with the current privacy and data protection frameworks.[27]

c) The Ministry of Corporate Affairs (**MCA**): In March 2021, the MCA asked all companies in India to disclose details about transactions (investment/deposits/trading) involving crypto or virtual currencies.[28]

d) Private banks in India have engaged fintech firms to explore blockchain based solutions. The report recommends public sector banks to also explore similar innovative solutions[73].

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

IT Act:

Section 2 (1) (za): an "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

Section 43A (Compensation for failure to protect data) explains: a "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

[***NOTE:*** *Obligations applicable to body corporates to manage personal and sensitive personal data are listed in the SPDI Rules.*]

PDP Bill:

Clause 3 (Definitions):

1) "Data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.

2) "Data principal" means the natural person to whom the personal data relates.

[73] See https://dea.gov.in/sites/default/files/Report%20of%20the%20Steering%20Committee%20on%20Fintech_1.pdf, p. 52.

3) "Data processor" means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary.

NPD Committee Report:

1) Clause 7.2 (ii): A "Community" is defined as any group of people that are bound by common interests and purposes, and involved in social and/or economic interactions. It could be a geographic community, a community by life, livelihood, economic interactions or other social interests and objectives, and/or an entirely virtual community.

2) Clause 6.1: A "data business" is any organisation that collects, processes, stores or manages both personal and non-personal data. A data business could be either a data custodian or a data processor or a data trustee.

3) Clause 7.4: A "data custodian" undertakes collection, storage, processing, use, etc., of data. Both the government and private entities can act as data custodians. A data custodian has a duty of care towards the concerned community to which the data pertains.

4) Clause 7.5: A "data processor" means a company that processes data on behalf of a data custodian.

5) Clause 7.7: A "data trustee" means an organisation, either Government organisation or a Non-profit Private organisation, that is responsible for the creation, maintenance and data-sharing of "high-value datasets". A data trustee also has a duty of care towards the concerned community to which the data pertains.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

SPDI Rules:

Rule 2 (1) (i): "Personal information" is considered any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a corporate body, is capable of identifying such a person, under Rule 2(1) (i).

Rule 3: "Sensitive personal data or information" of a person means such personal information which consists of information relating to:

1) password,

2) financial information such as bank account, credit or debit card or other payment instrument details,

3) physical, physiological and mental health condition,

4) sexual orientation,

5) medical records and history,

6) biometric information.

Rule 2 (1) (b): "Biometrics" refers to the technologies that measure and analyse human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes,

1) any detail relating to the above clauses as provided to corporate bodies for providing service, and

2) any of the information received under above clauses by corporate bodies for processing, whether stored or processed under lawful contract or not, provided that any information that is freely available or accessible in public domain or furnished under the 2005 Right to Information Act, or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

PDP Bill

Clause 3 (28): "Personal data" refers to data about or relating to a natural person who is directly or indirectly identifiable with regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.

Clause 3 (36): "Sensitive personal data" means personal data, which may reveal, be related to or constitute:

1) financial data,

2) health data,

3) official identifier,

4) sex life,

5) sexual orientation,

6) biometric data,

7) genetic data,

8) transgender or intersex status,

9) caste or tribe,

10) religious or political belief or affiliation or

11) any other data categorised as sensitive personal data.

Clause 33 (2), Explanation: ...The expression "critical personal data" means such personal data as may be notified by the central government to be the critical personal data.

Clause 91 (2), Explanation: ..."Non-personal data" means data other than personal data.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

There is nothing to this effect under the IT Act or the rules issued under it.

PDP Bill:

Clause 3 (2): "Anonymisation," in relation to personal data, is defined as an irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified which meets the standards of irreversibility specified by the DPAI.

Clause 3 (3): "Anonymised data" means data which has undergone an anonymisation process.

Clause 2 (B): The provisions of the act shall not apply to processing of anonymised data, other than anonymised data referred to in Clause 91 as follows:

1) Nothing in the act shall prevent the Central Government from framing any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such a policy does not govern personal data.

2) The Central Government may, in consultation with the (DPAI), direct any data fiduciary or data processor to provide any anonymised personal data or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in the manner prescribed.

[*Note: Reportedly, there are changes suggested to this clause by the committee of the Indian Parliament examining the PDP Bill.*]

Clause 38 (b): In cases where the processing of personal data is necessary for research, archiving, or statistical purposes, and the (DPAI) is satisfied that the purposes of processing cannot be achieved if the personal data is anonymised, it may, by notification, exempt such class of research, archiving or statistical purposes from the application of any of the provisions of this act as may be specified by regulations.

Pseudonymisation is not defined.

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

The provisions of the IT Act would apply to blockchain technology. If the relevant application collects personal and/or sensitive personal data, it would also have to comply with the SPDI Rules which directly deal with data protection. Also, if the relevant application acts as an intermediary as defined in the IT Act, it would also have to comply with the Information Technology (Intermediaries Guidelines and

Digital Media Ethics Code) Rules, 2021 (**Intermediary Rules**).[74] The Intermediary Rules require intermediaries to publish privacy policies, inform users to not deal with information that's invasive of another person's privacy and that it has the right to (1) terminate the access rights the user or (2) remove information, in the event the same violates the privacy policy of the intermediary.

Clause 2 (1) (w), IT Act: an "intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits a record or provides any service with respect to a record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-marketplaces and cyber cafes.

Going forward, when the PDP Bill becomes law, blockchain based applications dealing with personal data, sensitive personal data or critical personal data (as eventually defined under the law) will also have to comply with that law. The PDP Bill will then embody the data privacy framework applicable to the entire country.

The government is intending to introduce a law regulating crypto-currencies. A bill titled The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021 is listed in the agenda for the winter session of the Indian parliament (29 November to 23 December 2021).[31] Reports suggest that the Bill seeks to prohibit all private cryptocurrencies; except for certain exceptions. The contents of this Bill are not known yet and the Bill is yet to be introduced in the Parliament. Previously, in 2017, a high level inter-ministerial committee submitted a draft of the bill titled Banning of Crypto-currency and Regulation of Official Digital Currency Bill, 2019.[32] This draft Bill proposed a complete prohibition on the use of cryptocurrencies. But this Bill was not tabled in the Parliament.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

The Srikrishna Committee which drafted one of the earlier versions of India's personal data protection law, advised in its report against setting prescriptive standards as to what would constitute anonymisation. It argued for a contextual approach to carefully design and select anonymisation techniques specific to each use case. Such efforts should be based on the principle that different types of anonymised data pose varying degrees of re-identification risks. It would therefore fall on the DPAI to formulate adequate norms on what constitutes anonymised data, and routinely update such norms to accommodate technological advancements.

The NPD Committee Report discusses some anonymisation techniques for reference. These include K-anonymity, L-diversity, T-closeness, Amnesia, Anonimatron and Differential Privacy.

---

[74] See https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_15178073240777&type=rule&filename=Information%20Technology%20(Intermediaries%20Guidelines)%20Rules,%202011.pdf.

Unlike the UK ICO,[75] the Personal Data Protection Commission of Singapore[76], and the Working Party under article 29 of the EU Directive,[77] so far, no dedicated directives on anonymisation techniques and standards have been released by any regulator in India.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

SPDI Rules (Rule 7):

A body corporate can transfer sensitive personal data to any entity located in any other country, that ensures the "same level of data protection" that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

RBI Regulations:

Presently, data localisation requirements are applicable only to payments data. The RBI in a circular dated 6 April 2018 entitled "Storage of Payment System Data", [78] states that "All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details, information collected, carried, and/or processed as part of the message or payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required."

In April 2021, the RBI barred American Express and Diners Club from onboarding new domestic customers on their card networks for not storing payments data locally.[37] Similarly, it restricted Mastercard Asia from on-boarding new domestic customers (debit, credit or prepaid) onto its card network from July 22, 2021, for failure to comply with data localisation norms and to submit related audit reports.

After discussions, RBI has reportedly agreed to make some concessions on its data localisation requirements. Now, multinational banks can store certain details abroad, like name and address of the users or date, amount, name of the beneficiary and the reference number. However, the remaining details, like the purpose of the remittance and the mobile number of the users, must be stored locally.[38] RBI has allowed these relaxations so that global banks could implement their risk mitigation strategies efficiently. Such banks maintain their software for analysing AML/CFT risk at a central global hub and need to pool payments data from different countries to undertake the risk assessment.

PDP Bill:

Data localisation is envisaged in the PDP Bill. The current version of the PDP Bill states that (i) "critical personal data" may only be processed and stored in India

[75] See https://ico.org.uk/media/1061/anonymisation-code.pdf.
[76] See https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf.
[77] See https://www.dataprotection.ro/servlet/ViewDocument?id=1085.
[78] See https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244.

(clause 33 (2)), subject to the exceptions of providing health and emergency services, or where the central government has explicitly allowed such transfer; (ii) "sensitive personal data" may be processed outside India subject to certain safeguards listed in the PDP Bill, but must continue to be stored in India (clause 33 (1)).

Under clause 34 of the PDP Bill, the safeguards for processing sensitive personal data outside India are (A) The data principal must have given their explicit consent; and (B) (i) the transfer must have been made pursuant to a contract or intra-group scheme approved by the DPAI; or (ii) the central government, after consulting with the DPAI must have allowed the transfer to a country, entity or class of entities in a country or international organisation; or (iii) the DPAI must have allowed the transfer of the sensitive personal data or class of sensitive personal data for a specified purpose.

Under the PDP Bill, there is no requirement to locally store personal data (which is not sensitive or critical).

NPD Committee Report:

The NDP Committee Report recommends that non-personal data derived from personal data shall inherit the sensitivity of the underlying person data for storage requirements envisaged in the PDP Bill:[39]

1) Sensitive non-personal data may be transferred outside India but shall continue to be stored within India.

2) Critical non-personal data (which will follow the definition of Critical Personal Data which is to be notified by the Central Government) can only be stored and processed in India.

General non-personal data may be stored and processed anywhere in the world.

10. Is it necessary to notify processing activities to any authorities?

There is nothing to this effect under the IT Act or the rules issued under it.

PDP Bill:

The PDP Bill does not require regular "data fiduciaries" or "data processors" to report their processing activities to any authority, however, it lists certain additional compliances for "significant data fiduciaries" (**SDF**).

The DPAI may classify any data fiduciary or class of data fiduciaries as an SDF after considering, amongst other things, the volume of personal data they process, the sensitivity of personal data they process, their turnover, any risk of harm by processing, use of new technologies for processing and any other factor causing harm from such processing (Clause 26).

The additional compliances applicable to SDFs are: (i) registration with the DPAI; (ii) undertaking data protection impact assessment (**DPIA**) for certain processing activities; (iii) maintaining records as specified by regulations issued by the DPAI;

(iv) undergoing audit of policies and conduct of processing by an independent auditor; and (v) appointing a data protection officer (**DPO**).

The DPIA in turn should contain a detailed description of the proposed processing operations, the purpose of processing and the nature of personal data being processed, an assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed, and measures for managing, minimising, mitigating or removing such risk of harm. The DPIA is subject to review by the DPO. Further, the DPAI may direct the SDF to cease processing if it believes that such processing would cause, or is likely to cause, significant harm to data principals.

NPD Committee Report:

The NPD Committee has recommended the registration of "Data Business" having a certain data threshold. While the data threshold has not been specified, the NPD committee recommends considering factors such as gross revenue, number of consumers, households, device handled, revenues from consumer information, etc.[40] However, a voluntary, one-time, disclosure-based registration is envisaged, rather than a licence-based, compliance mechanism.[41]

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

IT Act and rules issued under IT:

Under the IT Act, if a corporate body that possesses, deals with or handles any sensitive personal data or information in a computer resource which it owns, controls or operates, neglects to implement and maintain reasonable security practices, and causes wrongful loss or wrongful gain to any person, then such person may claim compensation from the corporate body (section 43A).

Under the SPDI Rules, every person who provides information to a corporate body must be able to access a privacy policy which outlines the types of personal or sensitive personal data collected by the corporate body and the purposes for which such information is collected and used (Rule 4).

Further, sensitive personal data may be collected from persons only after obtaining their consent in writing (Rule 5 (7)). The person must also be given an opportunity to refuse or withdraw their consent (Rule 5 (7)). Lastly, consent should be obtained from principals before disclosing her information to any third party (Rule 6).

Also, individuals have the right to access and seek rectification of their sensitive personal data (Rule 5 (6)).

PDP Bill:

Under the PDP Bill, data principals are given more defined rights. These rights are:

- Clause 17 – Right to confirmation and access, i.e., right to confirm whether the data fiduciary is processing or has processed the data principal's

personal data, the data principal's right to access their personal data that the data fiduciary has processed or its summary, and the data principal's right to a brief summary of processing activities undertaken by the data fiduciary.

- Clause 18 – Right to correction and erasure, i.e., the right of the data principal to correct any inaccurate or misleading personal data, complete any incomplete personal data, update any out-of-date personal data and erase any personal data which is no longer necessary for the purpose for which it was processed. In the context of blockchain technology, this will likely take the form of a correcting/updating entry, while a record of the old entry will also remain.

- Clause 19 – Right to data portability, i.e., the right of the data principal to receive the following data in a structured, commonly used and machine-readable format – (i) personal data provided to the data fiduciary; (ii) the data generated in the course of provision of services or use of goods by the data fiduciary; or (iii) data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained. Further, it includes the right to have all this data transferred to any other data fiduciary in a machine-readable format.

- Clause 20 – Right to be forgotten, i.e., the right to restrict or prevent continued disclosure of the data principal's personal data by the data fiduciary under certain circumstances. This right is also contained in Clause 9 of the PDP Bill, which put a restriction on retention of personal data by data fiduciaries, unless the data principal provides consent. In the context of blockchain technology, this may either take the form of anonymisation, permanent masking or developments in code/coding languages which allow select administrators to make amendments to the information stored on a blockchain.

- Clause 53 – Right to file complaint with the DPAI against any data fiduciary if such data fiduciary has contravened the provisions of the PDP Bill (when it is enforced as an act).

Right to be forgotten:

So far, the right to be forgotten has not been recognised explicitly under any legislation. However, even in the absence of a statute, different courts have discussed the right to be forgotten, and recognised it in certain cases, though not as an absolute right. For instance, in 2019, the Delhi High Court[42] recognised the right to be forgotten and the right to be left alone as an inherent aspect of the fundamental right to privacy. Earlier, in 2017, while declaring the right to privacy as a fundamental right, the Supreme Court[43] observed that the right to control the dissemination of personal information should not amount to a right of total erasure of history. It opined that such a right cannot be exercised where the information or data is necessary, for exercising the right of freedom of expression and information, for compliance with legal obligations, for the performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical

research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

Users who part with their personal data on blockchain-based applications will qualify as data principals. In addition, nodes which process personal data in the manner listed in Clause 3 (31) of the PDP Bill (reproduced in Question 4 of this Chapter) will likely qualify as data processors. However, it is difficult to determine who the data fiduciary is among the developer, governing body, miners, nodes or participants.

Any person, including the State, a company or any juristic entity who determines the "purpose" and "means" of processing such personal data will qualify as a data fiduciary. Interestingly, if every participant on the blockchain network can contribute to its governance (by voting, surveys, etc.) then there is a risk of every participant qualifying as a data fiduciary. On the other hand, if the purposes and means of processing are determined by a dedicated governing body then only this governing body would be considered the data fiduciary.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The IT Act, the rules issued under it, and PDP Bill would apply to permissioned and permissionless blockchain networks alike.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

Currently, there are no laws/regulations/guidance/opinions in place which are directed at imposing limits on use, transfer and storage of data on public blockchains specifically.

Transfer and storage of data will be dealt in the manner discussed in Question 9 of this Chapter.

PDP Bill:

Depending on who is considered as the data fiduciary in a public blockchain, they will be subject to transfer, store, usage restrictions. They must process data for clear, specific, and lawful purposes only (Clause 4) and not process it for any other purpose (Clause 5). They must also collect the data only to the extent that is necessary for the purpose (Clause 6) and must retain it only for a period that's necessary to satisfy the purpose (Clause 9).

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

Some good practices for processing personal data:

- **Privacy Policy:** Displaying a privacy policy that describes what personal data is collected/ processed, why and how. For transparency, the data subjects (to whom the personal data belongs) should be informed of the benefits and limitations of using the blockchain technology. Sufficient emphasis must be placed on the immutability and the distributed nature of the blockchain and its privacy implications (such as the implication on the right of the data subjects).

- **On-chain and Off-chain processing:** While processing data, it is recommended that personal data is bifurcated into two data sets – (1) data set that is absolutely necessary to be processed on-chain; and (2) data set that can be processed off-chain. Accordingly, personal data that can be processed off-chain, should not be processed on-chain. Such that individuals can seek rectification or erasure of that data, if required.

- **De-identification and pseudonymisation:** For the personal data that is absolutely necessary to be processed on-chain, it is recommended that such data be de-identified or pseudonymised.

- **Encryption:** If it is necessary to process personal data on-chain (without de-identification or anonymisation), then it is recommended to encrypt the personal data while processing it on-chain. Further, sufficient and appropriate access control mechanisms should be implemented to control the access over the decryption key.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

The FATF's "travel rule" has not been implemented into the AML legislation.

Israel

Author

Smadar Peleg, Efficient Frontier

INATBA report, date written December 14, 2021, Smadar Peleg, Adv.

1. What are the legal acts regulating data privacy in your jurisdiction?

Privacy Protection Law, 1981.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

Ministry of Justice – The Privacy Protection Authority.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

Israel's first notable reference to cryptocurrencies is in its Tax Authority statement – Income Tax Circular No. 2018/05 – Tax Authority Subject: Taxation of activity by means of distributed payment (referred to as "virtual currencies", January 2018), which first guidance in highlighting that cryptocurrencies, for tax purposes, are an asset, similar to a stock. Therefore tax shall be paid in accordance to Capital Asset regulations – 25% tax on actual profit, meaning after conversion of the asset.

The Amendment from March 2021 to the Anti-Money Laundering Order (Obligations to identify, report and manage registrations of currency service providers for the prevention of money laundering and terrorist financing), 2014, Penalties and Criminal Law – Offenses – Prohibition of Money Laundering – Identification, Reporting and Management – defines "virtual currency" (a term not previously defined in legislation), "virtual currency wallet address" and "transaction amount" in a virtual currency.

Further the amendment effective from November 14, 2021 makes mandatory that each person receiving service in Israel, by a Financial Asset Service Provider ("FASP") must undergo a KYC process, and each Israeli FASP must report activity and suspicious activity reporting ("SAR").

The purpose of the current amendment to the order is to apply the money laundering regime to financial asset service providers as well, thus enabling them to act as additional significant players in the non-bank credit industry. The definition of FASP is amended to the order and now includes, inter alia, also the provision of services regarding "virtual currency", with the intention of supervising non-tangible financial services.

The Financial Services Supervision (Regulated Financial Services) Law, 2016 prohibits a person from engaging in providing a service in a financial asset unless

he holds a licence, also has been adjusted to "virtual currency" defining a Financial Asset Service Provider who is obligated to maintain a licence for this activity.

Currently, no company has received such a licence, and the only two Israeli companies who are working in accordance with the terms of this legislation, have received their right based on working before such legislation took effect. However several law firms in Israel are working with the authority to obtain such a licence.

4. What kind of actors (e.g., data subjects, controllers, processors...) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

There are no specific guidelines applying to data protection. Besides said authorities, currently the banks, specifically Israel's Central Bank ("Bank of Israel") has no guidelines on virtual currency, and since all banks have obligations based on the new orders, it is very difficult to open a bank account associated with virtual currency.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

"Sensitive information" is defined as data on a person's personality, the secrecy of his living, his state of health, his financial situation, his opinions and beliefs; and information determined by the Minister of Justice in an order.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

[Answer has not been provided.]

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

In accordance with the regulations of the AML Order, a customer who makes a transaction in a cumulative amount of more than NIS50,000 over a period of six months, will be asked to present an ID card and answer a number of questions in addition to the information required before applying – to the FASP.

A person who engages in providing a service in a financial assets or in the provision of credit without a licence, to provide a service in a financial asset or a licence to provide credit, as the case may be, is liable to imprisonment for 18 months or a fine at a rate three times the fine prescribed in section 61 (a) (4) of the Penal Code, and if the offence was committed by a corporation – double the said fine.

A new proposed law from 2022 will obligate to report digital assets holdings worth over NIS 200,000 by individuals.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

[Answer has not been provided.]

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

Generally, in accordance with Obsolescence laws and the Tax Authority statements, as it pertains to financial criminal offences relating to the corporations, entities will choose to store client data and trading history for at least 6 to 7 years.

10. Is it necessary to notify processing activities to any authorities?

Yes, to the Tax Authority.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

[Answer has not been provided.]

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

[Answer has not been provided.]

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

Not directly, no.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

There are no specific guidelines applying.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

There is no specific reference for blockchain privacy laws.

Privacy Protection Law, 1981, defines what invasion of privacy is and in what situations it is justified. It states that the invasion of privacy is a civil tort – which allows for a claim for damages, as well as a criminal offence – with a maximum sentence of 5 years in prison.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

Yes, Israel has adopted FATF's recommendations several years ago in its Anti-Money Laundering Order (Obligations to identify, report and manage registrations of currency service providers for the prevention of money laundering and terrorist financing), 2014, Penalties and Criminal Law – Offenses – Prohibition of Money Laundering – Identification, Reporting and Management. AML procedures for VASPs have been updated this year, 2021.

Japan

Authors

Ken Kawai, Anderson Mori & Tomotsune

Takeshi Nagase, Anderson Mori & Tomotsune

Huan Lee (Henry) Tan, Anderson Mori & Tomotsune

Kai Ishikawa, Anderson Mori & Tomotsune

1. What are the legal acts regulating data privacy in your jurisdiction?

The Act on Protection of Personal Information (the "APPI") is the main legislative instrument regulating data protection in Japan. The APPI was last amended in 2015 and those amendments have been in effect since 2017. The amendments relate to international transfers of data and the extraterritoriality of APPI regulations. Additionally, on June 5, 2020, a bill for the revision of the APPI submitted by the Personal Information Protection Commission (the "Commission") passed the Diet.[79]

The revision of the APPI (the "2020 Revised Act") seeks to strike a balance between the use and protection of personal data in view of recent advances in technology and heightened awareness of the need to protect personal information, and addresses new risks associated with the increased distribution of data across borders.

The 2020 Revised Act provides a definition for "Pseudonymously processed information", being information relating to individuals that can be derived from the processing of personal information in a way that will not enable the identification of specific individuals without collation with other information, and is expected to strengthen the regulation of Personal Information Handling Business Operators. The 2020 Revised Act will come into full force on April 1, 2022.

Additionally, further amendments to the APPI (the "2021 Revised Act"), based on the Act on the Arrangement of Related Laws for the Formation of a Digital Society, which was promulgated on May 19, 2021, will also come into effect in phases from April 1, 2022.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

The Commission has supervisory powers over Personal Information Handling Business Operators (as discussed in further detail in our response to question 4.) based on the delegation of such powers from the Prime Minister.

[79] https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

No specific regulation, guidance or opinion on data protection in the area of blockchain have been issued.

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

Personal Information Handling Business Operators are subject to the APPI.

Article 2, Paragraph 5 of the current APPI defines a "Personal Information Handling Business Operators" as a business operator (whether individual or corporation) that utilises a Database of Personal Information for its business. The APPI does not expressly exclude non-residents or foreign entities.

It should be noted, however, that central government organisations, local governments, incorporated administrative agencies etc. and local incorporated administrative agencies should be excluded from the definition of the Personal Information Handling Business Operators. This is because these entities are specifically regulated by other laws under current legislation.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Article 2, Paragraph 6 of the current APPI defines "Personal Data" as Personal Information that constitutes a Database of Personal Information.

"Personal Information" is defined in Article 2, Paragraph 1 of the APPI as (i) information regarding a living person that would allow identification of that specific individual by name, date of birth or other description contained in such information (including such information that can easily be viewed together with other information, and subsequently enables the identification of the specific individual) or (ii) information containing an individual identification code, being information in the manner of characters, letters, numbers, symbols or other codes as prescribed by cabinet order. It should be noted, for the avoidance of doubt, that the definition of "Personal Information" encompasses personal information relating to non-Japanese individuals.

"Database of Personal Information" is defined in Article 2, Paragraph 4 of the current APPI as a collection of information containing systematically aggregated Personal Information (i) that enables the search and location of certain Personal Information using a computer (with a focus on computer-processed information) or (ii) that is systematically organised based on a specific rule, and enables the easy location of certain Personal Information by means other than the use of a computer.

"Special care-required personal information" falls within a different category. Under Article 2, Paragraph 3 of the APPI, special care-required personal information means personal information comprising a data subject's race, creed,

social status, medical history, criminal record, any fact of the subject having suffered damage from a crime, or other matters prescribed by cabinet order as information the handling of which requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the data subject.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

Article 2, Paragraph 9 of the current APPI defines "Anonymously processed information" as information relating to an individual produced from the processing of personal information in a manner that prevents (i) the identification of a specific individual through the following actions (based on the category of personal information set forth therein) or (ii) the restoration of personal information:

A. personal information falling under Article 2, Paragraph 1, Item (i) of the APPI: deleting part of descriptions etc. contained in the said personal information (including the replacement of such descriptions with other descriptions via a dynamic method that prevents the restoration of the said descriptions);

B. personal information falling under Article 2, Paragraph 1, Item (ii) of the APPI; deleting all individual identification codes contained in the said personal information (including the replacement of the said individual identification codes with other descriptions using a dynamic method that prevents the restoration of the said personal identification codes).

The APPI currently contains no definition of pseudonymisation. However, the 2020 Revised Act will define "Pseudonymously processed information" at Article 2, Paragraph 5 as information relating to an individual, derived from the processing of personal information in a manner that prevents the identification of a specific individual without the collation of such information with other information through the following actions (based on the category of personal information set forth therein):

A. personal information falling under Article 2, Paragraph 1, Item (i) of the APPI; deleting part of the descriptions contained in the said personal information (including the replacement of such descriptions with other descriptions via a dynamic method that prevents the restoration of the said descriptions)

B. personal information falling under Article 2, Paragraph 1, Item (ii) of the APPI; deleting all individual identification codes contained in the said personal information (including the replacement of the said individual identification codes with other descriptions using a dynamic method that prevents the restoration of the said personal identification codes).

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

In light of the need for data protection, the Financial Service Agency, the supervisory authority in respect of the financial industry, has issued APPI guidelines specifically for the financial industry.

A blockchain business that is categorised as falling within the financial industry, such as a crypto asset exchange business, will be subject to such guidelines. The guidelines are generally stringent. For example, the guidelines require financial institutions, when notifying data subjects of the purposes for which their personal data will be used, to do so in writing.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

The Commission has issued guidelines on anonymisation techniques (although we note that the guidelines do not specifically refer to blockchain technology). For details of the techniques, please refer to Section 4 of the "Report by the Personal Information Protection Commission Secretariat: Anonymously Processed Information"[80]. Additionally, the Commission issued guidelines on pseudonymisation which contain Q&A about pseudonymisation techniques, measures to secure pseudonymously processed information etc.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

There is no legal requirement for personal data to be stored in Japan as a general matter. With that said, Article 19 of the current APPI requires Personal Information Handling Business Operators to strive to keep personal data accurate and up to date to the extent necessary to achieve the purposes for which the personal data will be utilised, and to delete personal data without delay when their utilisation has become unnecessary.

In addition, Article 20 of the current APPI requires Personal Information Handling Business Operators to take such action as necessary and appropriate to ensure the security control of personal data, including preventing the leakage, loss or damage of the personal data they handle. For example, the Ministry of Economy, Trade and Industry has published the Information Security Management Guidelines on the Use of Cloud Services to store personal data, in view of the security concerns involved in such a method of storing personal data. The guidelines address, among others, access control, data back-up, and employee management issues.

The APPI restricts the international transfer of personal data without a data subject's prior consent. However, an international transfer without the data subject's prior consent would be permitted if (a) the overseas transferee is located in a country that has a level of data protection that is equivalent to the personal data protections available in Japan (with the EU jurisdictions being the only jurisdictions that currently meet this requirement), and (b) an agreement ensuring compliance with the data protection standards in Japan has been entered into with the overseas transferee.

[80] https://www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf.

10. Is it necessary to notify processing activities to any authorities?

The APPI imposes no regular reporting obligation on Personal Information Handling Business Operators.

It should be noted, however, that the Commission is empowered under Article 40 of the APPI (to the extent necessary to implement the provisions of the APPI) to require Personal Information Handling Business Operators to submit such information or materials relating to their handling of personal information as the Commission deems necessary, or have its officials enter the relevant premises of Personal Information Handling Business Operators to inquire about their handling of personal information or to conduct inspection of their books, documents and other properties.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

Data subjects have the right under Article 27, Paragraph 2 of the current APPI to require Personal Information Handling Business Operators to provide information on the purposes for which retained Personal Data will be utilised. Personal Information Handling Business Operators, on their part, are in principle required to comply with such requests from data subjects without delay.

Under Article 28 of the current APPI Data subjects have the right to demand the disclosure of retained Personal Data by Personal Information Handling Business Operators. Personal Information Handling Business Operators, on their part, are in principle required to comply with such demands from data subjects without delay.

Under Article 29 of the current APPI, data subjects have the right, where the contents of retained Personal Data are not factual, to demand for Personal Information Handling Business Operators to make corrections, additions or deletions in relation to the contents of the retained Personal Data.

Furthermore, under Article 30, Paragraph 1 of the current APPI, data subjects have the right, where retained Personal Data is being handled in violation of the provisions of Article 16 of the current APPI (which provides for restrictions on the usage of personal data due to the purposes for which such data are being utilised) or where retained Personal Data had been acquired in violation of the provisions of Article 17 of the current APPI (which regulates proper acquisition of personal data), to demand for Personal Information Handling Business Operators to delete or cease their utilisation of retained Personal Data.

Separately, data subjects have the right, under Article 35, Paragraph 5 of the 2021 Revised Act, to request for Personal Information Handling Business Operators to suspend their use of Personal Data or suspend the provision of such Personal Data to third parties in situations where (a) there is no longer a need for the Personal Information Handling Business Operators to use the retained Personal Data, (b) the situation prescribed in the main clause of Article 26, Paragraph 1 (Leakage etc. of the Personal Data) pertaining to the relevant retained Personal Data has arisen,

or (c) there is a risk that the rights or legitimate interests of the data subject will be harmed by the handling of the retained Personal Data. In principle, the relevant Personal Information Handling Business Operator will be required, where such a request is deemed justified, to suspend its use of the said retained Personal Data or to suspend its provision of such data to a third party without delay and to the extent necessary, to avoid infringing the rights and interests of the relevant data subject.

However, neither the 2020 Revised Act nor the 2021 Revised Act contains any provision in respect of the right to be forgotten.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

It is believed that a Personal Information Handling Business Operator that records the Personal Information of its users on a blockchain (regardless of whether such usage is of the public permissionless or private and permissioned nature) would be the party regulated/responsible under the APPI.

In this connection, we believe that it would be difficult for a Personal Information Handling Business Operator to comply with the APPI if it records the Personal Information of its users on a public permissionless blockchain. As public blockchain involves the sharing of a database among unspecified participants, the use of blockchain technology may trigger the application of the APPI if information on the blockchain will not in principle be deleted or retracted once uploaded on the blockchain. For example, Article 19 of the current APPI requires Personal Information Handling Business Operators to delete unnecessary personal information once the purpose for which such personal information is required has been achieved. However, a Personal Information Handling Business Operator that records the Personal Information of its users on a blockchain may have difficulty deleting such information, and this could result in a violation of the APPI. In addition, if a Personal Information Handling Business Operator records the Personal Information of its users on a public permissionless blockchain, it would likely be in violation of Article 24 of the current APPI (which restricts the international transfer of personal data without a data subject's prior consent) and / or Article 16 of the current APPI (which restricts the usage of personal data based on the purposes for which such data are being utilised).

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

Please refer to our response to question 12. A Personal Information Handling Business Operator may be able to comply with the APPI if a private and permissioned blockchain with functions to satisfy the requirements of the APPI is used.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

Under Japanese laws and regulations, there are no particular restrictions on the use, transfer and storage of data using public blockchains. However, certain matters should be noted. For example, under the APPI, a business operator handling personal information must endeavour to erase personal data without delay when it is no longer necessary to use the data, or respond to a request from the individual to correct erroneous or inaccurate data. In this regard, due to the fact that it is virtually impossible to falsify information on a public blockchain, it would be difficult to erase or correct information recorded on a public blockchain. This makes it difficult to comply with the requirements of the APPI.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

Considering the characteristics of the public blockchain in which information recorded in one node is shared by an unspecified number of other nodes, it may be difficult to manage personal information through public blockchains in full compliance with the APPI. Therefore, at present, there is no default practice established for recording and managing personal information on a public blockchain.

On the other hand, if a private blockchain or a consortium-type blockchain is used, where the affiliation and attributes of the nodes that record and manage personal information are clear, it may be possible to use personal information in a way that complies with the APPI. However, it is uncommon to record and manage personal information even on private blockchains, and default practices have not yet been established.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

Currently, there is no legislation in Japan that corresponds to the FATF's travel rule.

However, the Japan Virtual and Crypto assets Exchange Service Association ("JVCEA"), a self-regulatory authority on crypto asset exchange service providers (“CAESP(s)”), has issued self-regulatory rules for CAESPs. These rules contain the equivalent of the FATF’s travel-rule on virtual asset service providers ("VASP"). There has been a proposal to amend the JVCEA's "Regulations on Anti-Money Laundering and Counter-Terrorist Financing in Relation to Crypto Asset Exchange Services" (the “Proposed JVCEA Rules”) for consistency with the FATF travel-rule, and the proposal is now under consideration.

Under the Proposed JVCEA Rules, if a CAESP that is a member of the JVCEA ("Japanese CAESP") receives a request from a user to transfer a crypto asset to an address managed by another CAESP, whether such CAESP is Japanese or otherwise (collectively, "CAESPs, etc."), it must obtain the following information from the requesting user and store such information before making any such transfer of crypto asset ("Crypto Asset Transfer to CAESP, etc."):

1. Information pertaining to the beneficiary

    a. crypto asset address to which the crypto asset will be transferred;

    b. information on whether the beneficiary is the person who requested the transfer, and if not, the name and address of the beneficiary (including, where the beneficiary is a corporation, its name and the location of its head or principal office); and

    c. name of (the receiving) CAESP, etc.

2. Other information necessary for assessing risks associated with the Crypto Asset Transfer to CAESP, etc. and information required to be obtained pursuant to the provisions of the Foreign Exchange and Foreign Trade Act of Japan and related regulations and guidelines (including but not limited to the purpose of the Crypto Asset Transfer to CAESP, etc.).

Russia

Authors

Maxim Lagutin, B-152

Maxim Zinovyev, B-152

Please note that this country's specific chapter has not been updated since the 2020 version of this report due to the ongoing situation in the region. The answer provided for the 2020 report has been reproduced below for your convenience.

1. What are the legal acts regulating data privacy in your jurisdiction?

Federal Law No. 152-FZ on Personal Data dated 27 July 2006 **(152-FZ)**, is a primary legal act regulating personal data processing in Russia.

There are certain Federal laws such as the Labor Code of the Russian Federation, "Federal Law No. 197-FZ" dated 30 December 2001, that determine specific processing situations (e.g., processing in the context of employment).

Federal Law No. 149-FZ, on "Information, Information Technologies, and Information Protection" dated 27 July 2006 **(149-FZ)** establishes basic rules for information processing.

Resolution No. 1119 of the Government of the Russian Federation, on "Approval of the Requirements to Data Protection in the course of Its Processing via Information Systems", dated 1 November 2012, determines the security measures for processing personal data via information systems.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

The Federal Service for Supervision of Communications, Information Technology and Mass Media **(Roskomnadzor)** is the main body responsible for supervision in the area of data protection.

The Ministry of Digital Development, Communications and Mass Media **(Mintsyfry)** is the regulator in regards to data protection.

The Federal Service for Technical and Export Control **(FSTEK)** determines technical and organisational measures for data controllers and is responsible for supervision in the area of information security, where it does not involve encryption.

The Federal Security Service **(FSB)** acts as the regulator in the area of information security, where encryption is involved.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

No specific documents have been issued in relation to blockchain.

The press noted that the regulator (Mintsyfry) was considering using the blockchain for certain business transactions, but at the date of this publication there were no official statements on this matter issued.

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

152-FZ mentions the following actors: "subjects of personal data" and "operators".

Pursuant to article 3 of the 152-FZ:

An "operator" (data controller) means a state body, a municipal body, a legal entity, or an individual which, alone or jointly with others organises and/or performs the processing of personal data, as well as determines the purposes of such processing, the content of personal data to be processed, and actions (operations) performed with personal data.

Although 152-FZ stipulates that an operator is entitled to assign the data processing to another person, the Law does not distinguish between an operator (data controller) and such another role (data processor). Pursuant to article 6 (3) of the 152-FZ, both the operator and the person acting on their behalf have the same duties, except for collecting data subject's consent (which is only the operator's duty). In practice, the operator is entitled to assign the collection of the data subject's consent to another person (data processor).

"Subject of personal data" (data subject) refers to a living natural person.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Pursuant to article 3 of the 152-FZ:

"Personal data" means any information relating to a directly or indirectly identified or identifiable natural person ("subject of personal data").

152-FZ specifically distinguishes between "special categories of personal data" and "biometric personal data" and states that processing of sensitive categories of personal data shall be prohibited unless certain conditions are met.

Pursuant to article 10 (1) of the 152-FZ, "special categories of personal data" include:

(a) personal data concerning racial or ethnic origin;

(b) personal data concerning political opinions;

(c) personal data concerning religious or philosophical beliefs;

(d) personal data concerning health;

(e) personal data concerning sex life or sexual orientation;

(f) personal data concerning criminal convictions;

152-FZ also specifically names "personal data made publicly available by a subject of personal data" (public data/publicly available data).

Pursuant to article 6 (10) of the 152-FZ, when a personal data subject (or a third party at the request of a data subject) makes their own data publicly available, a separate legal basis for the processing of such data is followed.

It should be noted, however, that according to a recent court ruling, there are certain criteria for qualifying personal data as publicly available data. For instance, in a case *VKontakte Social Network v. Double Data* the court suspended Double Data from extracting the information from Vkontakte's database without its permission.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

Yes.

Pursuant to article 3 (9) of the 152-FZ, "depersonalisation" (pseudonymisation) means "the processing of personal data in such a manner that personal data can no longer be attributed to a specific subject of personal data without the use of additional information".

In contrast to the GDPR definition of pseudonymisation, "depersonalisation" does not imply keeping respective additional information separate and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Although Russian legislation does not address irreversible anonymisation, following the logic of the definition of "personal data" the processing of anonymous data should not be subject to the provisions of the 152-FZ.

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

In recent years, Russian legislator (the State Duma) has developed several federal laws associated with the implementation of blockchain technologies:

- Federal Law No. 259-FZ, "On Raising Investments via Investment Platforms and on the Amendments to Certain Legislative Acts of the Russian Federation" dated 2 August 2019 (the **Crowdfunding Law**), which came into force on 1 January 2020, has introduced the use of utility tokens (referred to as digital utility rights as in the Law). The Crowdfunding Law does not address the use of cryptocurrencies or conducting ICO. In regards to exercising the utility tokens, the Crowdfunding Law limits the use of a

public permissionless blockchain network providing that the investment platform database is managed by the nodes.

- Federal Law No. 259-FZ "On Digital Financial Assets, Digital Currency and on the Amendments into Certain Legislative Acts of the Russian Federation" dated 31 July 2020 (the **Digital Financial Assets Law**) will enter into force on 1 January 2021, and is focused on using blockchain technology in the context of cryptocurrencies.

According to article 1 (7) of the Digital Financial Assets Law, "distributed ledger" (blockchain) is defined as a set of databases, the identity of the information contained in which is provided on the basis of established algorithms (algorithm).

The Digital Financial Assets Law also defines "nodes of information systems" which refers to the users of information systems based on a distributed ledger that ensures the identity of information contained in the specified information system, using procedures for confirming the validity of entries made or changed in it.

At the moment, there is no specific legislation referring to data privacy issues; conversely, it is currently premature to make conclusions about any implementation of blockchain technologies in any sphere of regulation.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

Yes.

Roskomnadzor issued "The Requirements and Methods of Depersonalization" by its Decree No. 996 dated 5 September 2013, and the "Guidelines for Applying Decree No. 996", dated 13 December, 2013.

The Decree only covers operators, which are either state or municipal bodies. Roskomnadzor explicitly claims that operators, which are legal entities or individuals, are prohibited from applying the methods (depersonalisation techniques) set in Decree No. 996. Conversely, companies use other techniques that are not mentioned in the Decree and claim that the resulting data is not "depersonalised data" and is rather just information that is not related to a natural person. Otherwise, the use of existing depersonalisation techniques by companies may be deemed unlawful by the supervisory authority.

There are four techniques mentioned in Decree No. 996:

A. "Introducing of identifiers" means replacing personal data values with identifiers and creating a table (reference list) matching identifiers with the original data;

B. "Changing the composition or semantics" means replacing personal data values with the results of generalisation or deletion of part of its values;

C. "Decomposition" means splitting a dataset into several subsets with subsequent separate storage of subsets;

D. "Permutation" means a rearrangement of individual records, as well as groups of records in the dataset.

At the moment, Roskomnadzor is developing a new set of techniques specifically for non-public operators (legal entities and individuals). As a member of the Center of Competence at Roskomnadzor, we participate in discussions concerning the development of depersonalisation techniques. In particular, we are trying to convince the supervisory authority to consider the existing methods of pseudonymisation and anonymisation mentioned in WP29 Opinion 05/2014 on Anonymisation Techniques, as well as ENISA's 2019 "Pseudonymisation Techniques and Best Practices".

However, it seems more likely that Roskomnadzor will not establish new techniques and will uphold those mentioned in Decree No. 996. Moreover, Roskomnadzor's viewpoint is that encryption and (or) hash function cannot be used for the pseudonymisation of personal data. It is difficult to change this position in practice because it is FSB, not Roskomnadzor, that solely controls encryption in Russia.

Provided that Roskomnadzor will establish the existing depersonalisation techniques for private use, we believe that it will not be relevant for blockchain-based applications and architectures. It will be fairly simple to trace back the transactions an individual has made because the techniques are not required to apply any security measures to keep the additional information private.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

Pursuant to article 18 (5) of the 152-FZ operators (regardless of their establishment), collecting personal data concerning Russian citizens shall use the databases located in Russia for recording, systemisation, accumulation, storage, correction (updating and modification) and retrieval of such personal data.

In its "Frequently Asked Questions"[81] regarding data localisation, the regulator (Mintsyfry) pointed out that it is permitted to duplicate databases concerning Russian citizens outside Russia, provided the original database (containing either a larger volume of personal data or equal to that located outside the territory of the Russian Federation) is stored in Russia.

As to international transfers, 152-FZ allows the transfer of personal data to adequate countries, which are:

A. parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (**Convention 108**);

B. ensuring adequate protection of the data subjects rights, provided that the legal provisions in force comply and the applicable security measures in the

[81] https://digital.gov.ru/en/personaldata/.

relevant state comply with the Convention 108. Roskomnadzor is responsible for establishing the list of such "adequate" countries by its Decree.

Transfers to countries that are not deemed to ensure adequate protection of personal data subject rights are permissible only on the following grounds:

1. The data subject has provided written consent for data transfer;
2. The processing is prescribed by international treaties of the Russian Federation;
3. The processing is prescribed by federal laws of the Russian Federation provided it is necessary to protect the foundations of the constitutional system of the Russian Federation, ensuring national defence and state security, ensuring sustainable and safe functioning of a transport complex, protection of the rights and freedoms of individuals, society and state in the sphere of transport complex from the acts of unlawful interference;
4. Processing is necessary for the performance of a contract to which the data subject is a party;
5. Processing is necessary in order to protect the vital interests of the data subject or of another natural person where the data subject is incapable of giving written consent.

10. Is it necessary to notify processing activities to any authorities?

Yes.

Before an operator commences personal data processing, it must notify Roskomnadzor on its intention to process personal data (article 22 (1) of the 152-FZ).

Pursuant to article 22 (3) of the 152-FZ, such notice shall contain the following information:

A. the identity and the address of the operator;
B. the purpose of data processing;
C. the categories of personal data concerned;
D. the categories of data subjects concerned;
E. the legal basis for the processing of personal data concerned;
F. list of actions (operations) performed with personal data and a general descrip- tion of the methods of data processing applied by the operator;
G. the description of technical and organisational measures applied by the operator including encryption and the name of such measures;

H. the name and contact details of the person responsible for data processing (data protection officer);

I. the commencing date of data processing;

J. the time period of data processing;

K. where applicable, transfers of personal data to a third country;

L. where the databases containing personal data concerning Russian citizens are located;

M. security measures applied.

The notice shall be submitted either by written or by electronic means.

152-FZ also provides certain exceptions from the notification requirement. This specifically includes when:

A. data is processed in the context of employment;

B. processing is necessary for the performance of a contract to which the data subject is a party or in order to enter into a contract with the data subject provided that personal data is not disclosed or provided to third parties without the consent of the data subject;

C. data relates to members of a public association or religious organisation and is carried out by such public association or religious organisation provided that personal data is not disclosed or provided to third parties without the written consent of the data subject;

D. data is made publicly available by the data subject;

E. data relates only to first name, last name, and patronymic;

F. processing is necessary for one-off admission of data subject to the operator territory;

G. data is processed by a state automated information technology system and state information technology system developed for the purpose of national security;

H. processing is not carried out by automated means;

I. data is processed in the context of transport security.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

According to articles 14–16 of the 152-FZ, a personal data subject has the right to:

A. access their own personal data

Data subjects are entitled to be informed about data processing, including confirmation of whether their data is being processed, the legal basis and purpos- es of data processing, the methods of data processing taken by the operator, the identity and location of the operator, the recipients of data, the categories of data concerned, from which source the personal data originate, time period of data processing, how to exercise the rights of the data subject, cross-border data transfer as well as the identity of the persons to whom data processing is assigned.

The operator shall provide such information to the data subject or their representative upon request.

The request must contain the details of the identity document of the data subject or its representative, information confirming the relationship with the operator (contract number, date of conclusion of the contract, conditional verbal designation, and (or) other information), or information otherwise confirming the data processing by the operator, and the signature of the data subject or its representative and may be submitted online (in which case it must be signed with a qualified advanced electronic signature) or by regular mail.

B. rectify their own personal data

Pursuant to article 14 (1) of the 152-FZ, the data subject has the right to request the operator to rectify personal data concerning them if it is incomplete, outdated, inaccurate, unlawfully obtained, or is not necessary for the stated purpose of processing.

C. erasure of personal data

Pursuant to article 14 (1) of the 152-FZ, the data subject has the right to request the operator to erase their personal data if it is incomplete, outdated, inaccurate, unlawfully obtained or is not necessary for the stated purpose of processing.

D. restrict the processing of personal data

Pursuant to article 14 (1) of the 152-FZ, the data subject has the right to request the operator to restrict the processing of their personal data if it is incomplete, outdated, inaccurate, unlawfully obtained or is not necessary for the stated purpose of processing.

E. object to direct marketing

Pursuant to article 15 of the 152-FZ, data processing for the purposes of promotion of goods and services on the market by making direct contacts with potential consumers through communication means, as well as for the purpose of political campaigning is only permissible when a data subject has given their consent.

Data subjects are entitled to object to such processing and the operator shall immediately stop processing activities.

F. object to decisions based solely on automated processing of personal data

Pursuant to article 16 of the 152-FZ, the data subject may be subject to a decision based solely on automated processing provided that they have given written consent or in case the processing is prescribed by federal laws establishing measures to safeguard the rights and the interests of the data subject.

Data subjects have the right to object to processing and the operator shall review the request within thirty days of its receipt and inform the data subject of the results of the review.

G. withdraw consent for data processing

Pursuant to article 9 (2) of the 152-FZ, the data subject has the right to withdraw their consent at any time.

The Law also provides that the operator may continue to process the data provided that there is another legal basis for such processing.

H. to lodge a complaint with Roskomnadzor or a court including claiming damages and (or) non-pecuniary losses

Pursuant to article 17 of the 152-FZ, in cases where the data subject believes that the operator processes their personal data in violation of the requirements of the 152-FZ or otherwise violates rights and freedoms, the data subject is entitled to lodge a complaint with Roskomnadzor or a court and claim damages and/or non-pecuniary losses.

The right to be forgotten does exist in Russia, but it is provided by 149-FZ, the law establishing basic rules on information processing.

Pursuant to article 10.3 of the 149-FZ, Internet search engines whose advertising targets consumers located in Russia shall remove links from its search results upon the request of a citizen (natural person) provided that the information concerning such citizen is distributed unlawfully, is inaccurate, outdated and has lost significance for such citizen except the information about criminal activity of such citizen which is still valid.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

In the absence of specific regulation on this matter, we suggest that the provisions on publicly available data may apply to the public permissionless blockchain network.

Pursuant to article 6 (10) of the 152-FZ, when a personal data subject (or a third party involved at the request of the data subject) makes their data publicly available, there is a separate legal basis for the processing of such data. Thus, this

legal basis may apply to public blockchains allowing any actors to collect, use or otherwise process such data.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The 152-FZ covers all data processing in Russia, as well as processing outside Russia where online activities target its territory including blockchain networks.

Due to a broad definition of "personal data"[82], the information related to transactions contained in the blockchain will likely be qualified as personal data. However, the context will determine the consequences of such qualification.

The participants in a private (permissioned) blockchain holding the information about data subjects will be considered operators and will thus be subject to duties imposed on the operator: to have a legal basis for such processing, to notify Roskomnadzor of such processing and to respect the rights of data subjects among others.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

[Answer has not been provided.]

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

[Answer has not been provided.]

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

[Answer has not been provided.]

[82] Any information relating to directly or indirectly identified or identifiable natural person ("subject of personal data").

Singapore

Author

Branson Lee, Blockchain Association Singapore

Dharma Sadasivan, BR Law Corporation

1. What are the legal acts regulating data privacy in your jurisdiction?

The Personal Data Protection Act 2012 (PDPA) sets the law on personal data protection in Singapore.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

The Personal Data Protection Commission (PDPC) is responsible for the administration and enforcement of the PDPA.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

Nothing specific has been issued in relation to blockchain.

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

The PDPA identifies the following actors: "organisations", "data intermediaries" and "individuals".

Pursuant to section 2 of the PDPA:

- "Data intermediary" means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation;
- "Individual" means a natural person, whether living or deceased;
- "Organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not:
    - (a) formed or recognised under the law of Singapore; or
    - (b) resident, or having an office or a place of business, in Singapore.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Pursuant to section 2 of the PDPA:

"Personal data" refers to data, whether true or not, about an individual who can be identified

A. from that data; or

B. from that data and other information to which the organisation has or is likely to have access.

The PDPA does not specifically categorise personal data into varying levels of sensitivity, such as "personal data" vs "sensitive personal data". However, the PDPC recognizes that different types of personal data can have different levels of sensitivity and also have the potential to result in varying levels of harm done to an individual in the event of a data breach. The onus is on organisations to provide a level of protection of personal data that is commensurate with the sensitivity of the personal data and potential harm that may result from a breach of that data.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

No. However, the PDPC has released a "Guide to Basic Data Anonymisation Techniques" **(the Anonymisation Guide)**[83], which introduces readers to data anonymisation concepts, techniques, methodology, risk assessments, technical controls, governance and more. The Guide itself is not part of the legislation and is not legally binding. However, it is indicative of how the PDPC will assess anonymisation or pseudonymisation efforts carried out by organisations.

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

Singapore is generally applying existing regulatory frameworks to blockchain technology. For example, the existing anti-money laundering regulatory framework applies to money laundering in the blockchain context. Similarly, if a digital token is considered a capital markets product then it will be regulated like other capital markets products under the Securities and Futures Act.

However, the Payment Services Act (**PSA**), which recently came into effect in January 2020 and establishes a comprehensive regulatory framework for the provision of payment services, expressly contemplates payment services relating to "e-money" and "digital payment tokens". The PSA does not, however, refer to data privacy.

Financial Services and Markets Bill 2022 (FSM Bill) was tabled for first reading in the Parliament on 14th February 2022. The MAS recognises the need for agility and effectiveness in addressing risks in the increasingly integrated financial sector. The key highlights for the bill include Prohibition Order, enhanced monitoring and regulation of VASPs in the areas of ML / CFT, power to issue directives to FIs regarding technology risk management including data protection and dispute resolution.

[83] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

The Singapore Courts and the PDPC have not endorsed any particular anonymisation or pseudonymisation techniques. However, as mentioned, the Anonymisation Guide is indicative of how the PDPC will assess anonymisation or pseudonymisation efforts carried out by organisations.

The Anonymisation Guide was also referenced in AIA Singapore Private Limited [2019] SGPDPC 20 (**AIA**), albeit in a rather narrow context.

In this case, AIA Singapore Private Limited, an insurance company, sent a bulk-posting of letters relating to the insurance policies of various policyholders. Due to a technical error in AIA's IT system, many of these letters ended up addressed to only two recipients. Thus, the two recipients received numerous letters containing the personal data of other policyholders.

AIA deployed a fix to rectify the error (the **Fix**) and conducted testing. AIA used one single address as the recipient address when testing the Fix, on the basis that using just one address would prevent disclosure of production data.

The PDPC held that this was inadequate. Using a single address would not reveal whether the technical error had been fixed, because the technical error occurred under specific circumstances where multiple addresses were involved. The PDPC also stated:

"There are proven ways to generate dummy or test data that reflects the distribution of the production data without resorting to using a single address, e.g., by swapping the data."

The PDPC further noted in a footnote that:

"The purpose of swapping is to rearrange the data in the dataset such that the individual attribute values are still represented in the dataset, but generally do not correspond to the original records. This technique is also referred to as shuffling and permutation. For more details, please refer to the Commission's Guide to Basic Data Anonymisation Techniques."

Therefore, while the PDPC has not gone so far as to endorse any specific anonymisation or pseudonymisation techniques, the AIA case suggests that the PDPC expects organisations to be familiar with the Anonymisation Guide and will reference it when assessing whether organisations have taken adequate steps to anonymise or pseudonymise personal data.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

The PDPA does not impose any positive requirement to store personal data locally.

However, section 26 of the PDPA prohibits the transfer of personal data out of Singapore except in accordance with the requirements of the PDPA, to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act (the **Transfer Limitation Obligation**).

Regulation 9(1)(b) of the Personal Data Protection Regulations 2014 (the **Regulations**) further requires transferors to take appropriate steps to ensure that recipients of the transferred personal data are bound by "legally enforceable obligations" to provide the transferred personal data standard of protection comparable to the protection under the PDPA. This suggests that a transfer of personal data under the Transfer Limitation Obligation contemplates and requires a recipient in respect of the transferred personal data.

Further guidance from the PDPC would be helpful for scenarios in which data has been moved outside of Singapore's borders but there is no recipient. For example, it is unclear if personal data has been "transferred" out of Singapore for the purposes of the Transfer Limitation Obligation if an individual brings a flash drive containing personal data overseas (e.g., in the individual's pocket) without ever handing over possession of the flash drive to a third-party.

10. Is it necessary to notify processing activities to any authorities?

Currently the PDPC does not require organisations to notify them of data processing activities.

However, for completeness, organisations are currently encouraged (but not required under the PDPA) to notify the PDPC of data breaches. A draft of the Personal Data Protection (Amendment) Bill, which was recently released for public consultation, contains a section that would make notification of data breaches mandatory under certain circumstances.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

Individuals have access and correction rights under the PDPA.

Access: Pursuant to section 21(1) of the PDPA, upon request, an organisation must provide the data subject, as soon as reasonably possible, with (i) personal data about the data subject that the organisation has in its possession or control; and (ii) information about how that personal data has been or may have been used or disclosed within one (1) year from the data subject's request.

Organisations are not required to provide access to an individual under certain exemptions as set out at the Fifth Schedule of the PDPA. The exemptions include, amongst others: opinion data kept solely for an evaluative purpose, personal data which is subject to legal privilege, personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation, personal data collected, used or disclosed without consent pursuant to exemptions for investigations or

proceedings if the investigation and associated proceedings and appeals have not been completed and requests that are frivolous, vexatious or pertain to trivial information.

Correction: Pursuant to section 22(1) of the PDPA, an individual is entitled to request an organisation to correct an error or omission in their personal data that is in the possession or control of that organisation. Upon receipt of the correction request, the organisation must correct the personal data as soon as practicable, and send the corrected personal data to every other organisation to which the personal data was disclosed within the preceding year from the correction date. This ensures that those third-parties are provided with the updated personal data.

Organisations are not required to correct personal data of an individual under certain exemptions as set out at the Sixth Schedule of the PDPA. The exemptions include, amongst others: opinion data kept solely for an evaluative purpose, any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results and documents related to a prosecution if all proceedings related to the prosecution have not been completed.

Right to be forgotten: The right to be forgotten, or right of erasure, does not currently exist in Singapore.

For completeness, it is necessary to note that section 25 of the PDPA requires organisations to cease retaining personal data, or remove the means by which the data can be associated with individuals (i.e., anonymise it), as soon as it is reasonable to assume that the purposes for which the personal data was collected are no longer served by its retention, and retention is not needed for legal or business purposes **(the Retention Obligation)**.

However, to be clear, the Retention Obligation is a direct obligation of the organisation – it is not a right exercisable by an individual allowing the individual to compel the organisation to cease retention of personal data.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

The PDPA does not address this and there is no specific guidance on this matter from the PDPC.

If an individual stores or uploads unencrypted personal data onto a public permissionless blockchain network after which no one party can exercise control over it and the personal data becomes available to all, that individual has essentially made the personal data publicly available. This can be seen as analogous to an individual publishing their personal data on the internet and making it publicly available. Under the PDPA, personal data which is publicly available can be collected, used and disclosed without the individual's consent.

Similarly, a third-party that uploads an individual's unencrypted personal data to a public permissionless blockchain network where it becomes publicly available would be analogous to a third party uploading personal data on the internet

where it becomes publicly available. If either is done without the individual's consent or without falling within an exemption from consent under the PDPA, the third party would be committing a data breach.

Further analogies can also be drawn for various scenarios on this basis.

However, it is more likely that where an organisation contemplates handling personal data on a blockchain network, it will use a private permissioned network so that the transactions are private and users are known and trusted, and with possible off-chain transactions to further segregate data or prevent data from being disseminated to the network.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The PDPA applies to all organisations resident in Singapore, as well as all organisations that collect, use, disclose or transfer out of Singapore, or otherwise store or handle personal data from Singapore. This would include organisations that are blockchain networks, regardless of structure.

The exact nature of how the PDPA applies will depend on the facts of each case. Some factors that may affect how the PDPA applies include which/whether any party exercises control over the personal data, which/whether any party processes personal data on behalf of another, whether any personal data is transferred out of Singapore, how personal data is protected on the network, how long the network retains personal data, what purposes require the collection, use, or disclosure of personal data on the network, etc.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

There are no specific discussions/ interpretations around this.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

We have seen experimentations of financial use cases using private blockchains. As for public chains, most wallets are pseudo anonymous without linkages to real world data except for centralised exchanges where FATF rule is followed closely by the regulators.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

Sharing of beneficiary information as well as confirmation of ownership of non-custodial wallets. VASP-VASP transfers are somewhat facing some sunrise

issues and at this moment there seem to be a few solutions in the market without a front runner as of now.

South Africa

Authors
Caitlin Gottschalk, Gottschalk Attorneys
Njabulo Kubheka, Gottschalk Attorneys
Kerry Bundy-Palmer, Gottschalk Attorneys
Patience Katiyo, Gottschalk Attorneys

1. What are the legal acts regulating data privacy in your jurisdiction?

South Africa has taken significant steps to implement laws and regulations relating to the protection of data and personal information. Below is a list of the legislations which regulate data privacy, together with the purpose for which such legislation was enacted.

1. The Constitution of the Republic of South Africa, 1996 ("Constitution")

   The Constitution guarantees the right to privacy to all people in the Republic under section 14 thereof.

2. The Protection of Personal Information Act 4 of 2013 ("POPIA")

   POPIA seeks to:

   a. give effect to the constitutional right to privacy by safeguarding personal information when processed by a Responsible Party, subject to justifiable limitations;

   b. regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

   c. provide persons with rights and remedies to protect their personal information from processing that is not in accordance with POPIA; and

   d. establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by POPIA.

3. Promotion of Access to Information Act 2 of 2000 ("PAIA")

   PAIA was enacted to give effect to the constitutional right of access to any information held by the State and any information held by private bodies that is required for the exercise and protection of any rights.

4. Electronic Communications and Transactions Act 25 of 2002 ("ECTA")

    a. ECTA is a law of general application which applies to transactions concluded electronically or by way of data messages.

    b. Chapter XIII of ECTA deals specifically with cyber-crime. Sections 85, 86, 87 and 88 of ECTA, amongst other things, states that a person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence under such legislation.

    c. ECTA seeks to:

        - provide for the facilitation and regulation of electronic communications and transactions;
        - provide for the development of a national e-strategy for the Republic of South Africa;
        - provide for the development of a national e-strategy for the Republic of South Africa; and
        - promote universal access to electronic communications and transactions and the use of electronic transactions.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

1. The South African Information Regulator ("Information Regulator"):

    The Information Regulator is an independent and impartial body established in terms of section 39 of POPIA. It is subject to the law and the Constitution and is accountable to the National Assembly. The Information Regulator is required to perform its function and exercise its powers without fear, favour, or prejudice.

2. The Role of the Information Regulator:

    a. The Information Regulator is empowered to monitor and enforce compliance by public and private bodies with the provisions of POPIA.

    b. The Information Regulator is also in charge of publishing codes of conduct for various industries and developing guidelines to aid entities in developing and implementing codes of conduct.

    c. These codes of conduct contribute to the proper implementation of the conditions for the lawful processing of personal information in each sector.

d. Further, these codes must specify how the conditions must be complied with within various industry sectors with regards to the processing of personal information.

e. The Information Regulator is responsible for receiving complaints from the public when there is a belief that their personal information is being compromised. These concerns may also be investigated by the Information Regulator.

f. It is also important to mention that the Information Regulator is further in charge of all the functions of the South African Human Rights Commission under the PAIA.

g. Apart from the courts, the Information Regulator is the only functionary that may consider complaints against decisions made by public or private organisations in response to requests for access to their documents.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

The Information Regulator has not issued any specific regulation, guidance or opinions regarding blockchain technology.

4. What kind of actors (e.g., data subjects, controllers, processors...) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

The following actors are identified in South Africa:

1.	Data Subject	means the person to whom personal information relates;
2.	Operator	means a person who processes personal information for or on behalf of a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party;
3.	Regulator	means the Information Regulator established in terms of section 39 of POPIA; and
4.	Responsible Party	means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

POPIA makes a distinction between "*Personal Information*" and "*Special Personal Information*". Special Personal Information also makes reference to "*Biometric Information*".

1. Personal Information

   Section 1 of the POPIA defines Personal Information as information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

   1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person;
   2. information relating to the education or the medical, financial, criminal or employment history of the person;
   3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
   4. the Biometric Information of the person;
   5. the personal opinions, views, or preferences of the person;
   6. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
   7. the views or opinions of another individual about the person; and
   8. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2. Special Personal Information

   Section 1 of POPIA defines Special Personal Information as Personal Information concerning:

   a. the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
   b. the criminal behaviour of a data subject to the extent that such information relates to:
      - the alleged commission by a data subject of any offence; or
      - any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

3. Biometrics

   Biometrics are defined as a technique of personal identification that is based on physical, physiological, or behavioural characterisation including

blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

1. The terms de-identification, anonymisation and pseudonymisation are, at times, used interchangeably. POPIA, however, makes use of the term "*de-identification*" for this purpose.

2. The definition of de-identification, in relation to a data subject, is the deletion of any information that identifies the data subject, can be used, or manipulated by a reasonably foreseeable method in order to identify the data subject or can be linked by a reasonably foreseeable method to other information that identifies the data subject.

3. POPIA does not apply to de-identified information which cannot be re-identified. The reason for this is that POPIA does not consider such information to be Personal Information.

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

1. At the date of providing this opinion, there is no official legislation or regulations specifically governing the use of blockchain technology.

2. The Intergovernmental Fintech Working Group ("IFWG") has, together with the Crypto Assets Regulatory Working Group ("CARWG"), published what is called a "position paper" on crypto assets which confirms that crypto assets will be brought into the South African regulatory review in a "phased and structured manner". The South African Reserve Bank has, however, confirmed that decentralised convertible virtual currencies such as Bitcoin, are not regarded as legal tender in South Africa.

3. The intention of the regulatory bodies in South Africa is to regulate the Crypto Asset Service Providers ("CASPS") as entities, rather than the crypto assets themselves. The position paper recommends that CASPS are to be included as an accountable institution in terms of the Financial Intelligence Centre Act 38 of 2001 ("the FAIS Act").

4. At this stage, there is little regulation regarding the use of blockchain technology and it remains a highly volatile and risky environment within South Africa. The use of blockchain and the mining of crypto currency is not prohibited in South Africa, however, there is no real recourse available to a person or entity that trades in such "currency" if things take a turn for the worse.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

To date, the Information Regulator, courts and experts on the subject have not addressed any specific and required anonymisation, pseudonymisation or as per POPIA, de-identification techniques. Should this be addressed in future, it will certainly be relevant to blockchain-based applications and technology due to the absolute need for safety and data protection in use of such applications.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

1. Storing personal data locally

   Although there is no absolute requirement in terms of POPIA, it is suggested that Personal Information should be stored locally, except for the provisions of section 72 whereby international or cross border information flow takes place.

2. International transfers

   a. The aim of POPIA is not to prohibit the sharing or flow of Personal Information in its entirety, but rather to ensure that sufficient safeguards are in place, by way of adequate legislation and regulations, that protect such outflow of Personal Information and the data subjects to which such information relates. This is in-line with international best practice.

   b. Where Personal Information is transferred outside South Africa, the Responsible Party must notify all affected persons that it intends to undertake such transfer to another country and further disclose the level of protection afforded to such information by the foreign country. This is in-line with international best practice as well as the intention of POPIA, in that even though this information is transferred out of the country, where POPIA may not apply, that Personal Information will still be given an adequate level of protection.

   c. In terms of Section 72, POPIA dictates that Personal Information can only be transferred to a foreign country in the following circumstances:

      - if the country to which the information is transferred, or subsequent transferee countries, have similar or adequate protection levels of Personal Information as afforded by POPIA in the form of legislation, binding corporate rules or a binding agreement;

- the entity or persons in such foreign country that receive such information agree to treat such Personal Information in a way similar to that provided for in POPIA;
- there is consent by the data subject, as defined in POPIA, for the transfer of such Personal Information;
- the transfer is absolutely necessary in terms of a contract between the data subject and the Responsible Party; or
- the transfer is in the interest or benefit of the data subject where it is not reasonably practical to obtain the consent of the data subject but that the data subject would have likely agreed to and given consent for such transfer.

10. Is it necessary to notify processing activities to any authorities?

1. The authority responsible for the proper administration of POPIA is the Information Regulator. Generally, it is not necessary to notify the Information Regulator on each and every data processing activity, however, there are certain instances in which prior authorisation from the Information Regulator is required.
2. Section 58 of POPIA places an obligation on the Responsible Party to notify the Information Regulator should the processing of any Personal Information be undertaken in terms of section 57, as discussed more fully below. The Responsible Party, in such instances, may not process such Personal Information until such time as the Information Regulator has completed an investigation into such a request or a notice is received by the Responsible Party that a more detailed investigation will not be conducted, allowing the data processing to continue.
3. In terms of section 57 of POPIA, a Responsible Party must obtain prior authorisation from the Information Regulator, if such party intends to:
    - process any unique identifiers of data subjects for a purpose other than that which it was originally collected and with the intention of linking such information with information collected by other responsible parties;
    - process information on criminal behaviour or on unlawful and objectionable conduct on behalf of third parties;
    - process information for the purposes of credit reporting;
    - transfer Special Personal Information, as per section 26, including information relating to a person's:
        i. religious or philosophical beliefs;
        ii. race or ethnic origin;
        iii. trade union membership;

iv. political persuasion;

v. health or sex life;

vi. biometric information;

vii. and criminal behaviour; or

viii. the Personal Information of children as referred to in section 34, to a third party in a foreign country that does not provide sufficient data protection of Personal Information.

4. This list is not exhaustive, and the Information Regulator may apply the above-mentioned rules to other information processing, by law or regulation, if such processing poses a particular risk to the legitimate interests of a data subject.

5. The Responsible Party is only required to obtain such prior authorisation once, unless the purpose for such processing has deviated from the original authority given to the Responsible Party.

6. The provisions of section 57 and 58 are not applicable if a code of conduct has been issued to a specific sector or industry.

7. A contravention of sections 57 and 58 of POPIA will result in the Responsible Party being guilty of an offence and liable to a penalty in the form of a fine and/or imprisonment not exceeding 12 (twelve) months.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

1. Section 5 of POPIA sets out various rights that are provided to data subjects which includes the rights to:

    a. be notified that Personal Information about him, her or it is being collected;

    b. be notified that his, her or its Personal Information has been accessed or acquired by an unauthorised person;

    c. establish whether a Responsible Party holds Personal Information of that data subject and to request access to his, her or its Personal Information;

    d. request, where necessary, the correction, destruction or deletion of his, her or its Personal Information;

    e. object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its Personal Information;

    f. object to the processing of his, her or its Personal Information at any time for purposes of direct marketing;

g. not to have his, her or its Personal Information processed for purposes of direct marketing by means of unsolicited electronic communications;

h. not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its Personal Information intended to provide a profile of such person;

i. submit a complaint to the Information Regulator regarding the alleged interference with the protection of the Personal Information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator; and

j. institute civil proceedings regarding the alleged interference with the protection of his, her or its Personal Information.

2. POPIA does not expressly provide for the right to be forgotten, which is basically a right to have private information about a data subject removed from internet searches and other directories under some circumstances.

3. POPIA rather states that Personal Information may only be stored to the extent that is adequate, relevant, and not excessive in relation to the purpose for which it was collected. This includes retaining information for only so long as it is required and not in excess of such a time period.

4. Section 24 of POPIA further provides that a data subject may request a Responsible Party to correct or delete Personal Information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully. Furthermore, POPIA provides that a data subject may request a Responsible Party to destroy or delete a record of Personal Information about the data subject that the Responsible Party is no longer authorised to retain.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

As stated above, there is no specific legislation regulating the blockchain actors in South Africa. POPIA does not provide any specific provisions dealing with how blockchain actors will be regulated, but rather requires all Responsible Parties to comply. The most relevant provisions which will be applicable to blockchain personal data controllers will be the provisions of POPIA.

There is merit in the argument that in the instance of a public permissionless blockchain, the data subject provides the required consent to the processing of his, her or its Personal Information by virtue of voluntarily placing such information on the blockchain. This subject shall require further ventilation which will only be possible through the development of legislation, regulation and case law.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

1. The purpose of POPIA is to give effect to the constitutional right to privacy, by safeguarding Personal Information when processed by a Responsible Party. The South African Constitution provides that the right to privacy binds all natural and juristic persons and all organs of state within the Republic of South Africa.

2. Despite the fact that blockchain technology is not expressly provided for in POPIA, it is submitted that the application of POPIA is implied, given the nature of the legislation and its purpose. It is however submitted that the application will be subject to the limitations provided in both POPIA and the Constitution. For example, there will be no data breach where a data subject provided consent for the Personal Information to be processed.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

1. As stated above, even though POPIA does not expressly provide for the application of its provisions to blockchains, there is a reasonable belief that POPIA will apply. Any party engaging with and operating within a public blockchain will be required to comply with the provisions of POPIA.

2. It is plausible that when a person places their Personal Information on a public blockchain, he or she, through such action, will have consented to the use and sharing of his or her Personal Information.

3. Case law and regulation will have to develop to take account of public blockchains in this regard.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

1. Prior to the enactment of POPIA, the commonly used practices for processing of personal data on both private and public blockchain was The Constitution, PAIA and ECTA.

2. PAIA was enacted to give effect to the constitutional right of access to any information held by the State and any information held by private bodies that is required for the exercise and protection of any rights. PAIA gives effect to processing of personal data on both private and public sector by:

    a. giving individuals and companies access to records which contain Personal Information about the data subject in both private and public sector;

b. requiring private and public sectors to take reasonable steps to create internal measures for the correction of Personal Information; and

c. prohibiting the disclosure of a record if it would involve unreasonable disclosure of Personal Information about third parties.

3. ECTA regulates electronic commerce in South Africa. The purpose of ECTA is to:

a. provide for the facilitation and regulation of electronic communications and transactions;

b. provide for the development of a national e-strategy for the republic of South Africa;

c. to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs;

d. to provide for human resource development in electronic transactions; to prevent abuse of information systems; and

e. to encourage the use of e-government services; and to provide for matters connected therewith.

4. Section 51 of ECTA deals with principles for electronically collecting Personal Information. This section provides that a data controller must have:

a. have the express written permission of the data subject for the collection, collation, processing, or disclosure of any Personal Information on that data subject unless he or she is permitted or required to do so by law;

b. may not electronically request, collect, collate, process, or store Personal Information on a data subject which is not necessary for the lawful purpose for which the Personal Information is required;

c. must disclose in writing to the data subject the specific purpose for which any Personal Information is being requested, collected, collated, processed, or stored;

d. may not use the Personal Information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law;

e. must, for as long as the Personal Information is used and for a period of at least one year thereafter, keep a record of the Personal Information and the specific purpose for which the Personal Information was collected;

f. may not disclose any of the Personal Information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject;

g. must, for as long as the Personal Information is used and for a period of at least one year thereafter, keep a record of any third party to whom the Personal Information was disclosed and of the date on which and the purpose for which it was disclosed;

h. must delete or destroy all Personal Information which has become obsolete; and

i. that a party controlling Personal Information may use that Personal Information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction?

1. South Africa is a member of both the FATF and its FATF-style regional body known as the Eastern and Southern Africa Anti-Money Laundering Group and is therefore obligated to implement its recommendations.

2. South Africa recognises cryptocurrency as an investment and taxable asset. The CARWG recommended that crypto-assets be declared a financial product through the provisions of the FAIS Act.

3. Section 8.4.2 of South Africa's IFWG 2020 Position Paper on Crypto Assets notes that crypto service providers will be required to register and observe all relevant provisions of the Financial Intelligence Centre Act 38 of 2001 ("FICA"), including requirements aimed at AML. This will include conducting customer identification and verification, conducting customer due diligence, keeping records, monitoring for suspicious and unusual activity on an ongoing basis, reporting any suspicious and unusual transactions, reporting cash transactions of R25 000.00 (twenty five thousand Rands) and above or the applicable threshold at any given time. Other obligations will include developing, documenting, maintaining and implementing a risk management and compliance programme, ensuring compliance with the FICA, and training employees on matters related to AML compliance.

4. In 2020, the Eastern and Southern Africa Anti-Money Laundering Group recommended that South Africa include a "travel rule", which forces countries to ensure that their VASPs share beneficiary and originator transmittal information with counterparts. South African policymakers have now demonstrated their intent to comply with this recommendation. The originator (sender) CASP and beneficiary (recipient) CASP are collected and

keep "required and accurate" originator and beneficiary crypto asset transmittal information and share this with the authorities when needed.

What kinds of personal data need to be shared by VASPs and what kinds of transactions are applicable?

1. The FATF Travel Rule requires VASPs to collect and share personal data during transactions. In South Africa, there are currently no promulgated laws or regulations that address the use of virtual currencies. This therefore means that there is currently no legal protection or recourse is afforded to users of virtual currencies.

2. There is currently a draft policy aimed at regulating virtual currencies. The policy is based on international requirements and includes the implementation of the FATF travel rule.

3. The draft regulatory framework implies that VASP's will be subjected to the requirements of the FICA, which will place an obligation on VASPs to collect Personal Information and documentation for its clients. The regulation of virtual assets will also ensure the integrity of the financial system and will demonstrate South Africa's commitment to combating financial crime.

South Korea

Authors

Kijun Kwon, Kwon, Park & Rhee

Jungyoon Oh, Kwon, Park & Rhee

Kwanhoo Oh, Kwon, Park & Rhee

1. What are the legal acts regulating data privacy in your jurisdiction?

In Korea, there are three laws related to personal information: the Personal Information Protection Act, the Act on Promotion of information and Communications Network Utilization and Information Protection (Information and Communication Network Act), and the Credit Information Use and Protection Act (credit Information Act). These three laws are collectively referred to as the 3 Data Act (Data Sam Bub).

The Personal Information Protection Act is a general law that protects the freedom, privacy, and rights of individuals from personal information leakage, misuse, and abuse, and further, to realise the dignity and value of the individuals, by prescribing the processing and protection of personal information. The Act on Promotion of Information and Communications Network Utilization and Information Protection is a special law that stipulates the protection of personal information in case of providing information and communication services using information and communication networks. The Credit Information Act is a special law that stipulates personal information protection in individual sections such as banking and finance.

The contents below deal with “the Personal Information Protection Act” unless otherwise mentioned.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

According to the revision of the Personal Information Protection Act in August 2020, the authority of regulation and supervision related to online personal information protection has been changed to the Personal Information Protection Commission affiliated with the Prime Minister. All functions related to personal information protection by the Korea Communications Commission and the right to investigate and dispose of general commerce corporates by the Financial Services Commission were transferred to the Personal Information Protection Commission. The Information and Communication Network Act is managed by the Ministry of Science and ICT and the Korea Communications Commission. The Credit Information Act is managed by the Financial Services Commission.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

Currently, there are no regulations that oversee the entire blockchain industry. However, the Ministry of Science and ICT has created "the guidelines for the introduction of blockchain technology to national public institutions" and presented the basic requirements for "authorised blockchains" as cryptographic technology.

Although it is not applied to the entire blockchain industry, the Act on Reporting and Using Specified Financial Transaction Information defines the meaning of virtual assets and the transactions; and requires virtual asset business operators to meet certain conditions (real name deposit account, information protection management system certification) and report to the Commissioner of Korea Financial Intelligence Unit. (See Q7). Through the revision of the Income Tax Act, laws and regulations required for taxation on virtual assets have been reorganised.

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

- The term “data subject” in the Personal Information Protection Act means an individual who is identifiable through the information processed and is the subject of that information (Article2, No 3).
- The term “personal information controller” means a public institution, legal person, organisation, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities (Article2, No5); If a personal information controller entrusts a third party with the processing of personal information, the trustee of the personal information processing is also included as a personal information controller (Article26, No2).
- The term “processing” means the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, searching, output, correction, recovery, use, provision, disclosure, and destruction of personal information and other similar activities (Article2, No2).

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

1. The Personal Information Protection Act
    - The term "personal information" means any of the following information relating to a living individual.
        i. Information that identifies a particular individual by his or her full name, resident registration number, image, etc.;

ii. Information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual (Article2 No.1).

- "Sensitive information" is information on ideas and beliefs, membership and withdrawal of labor unions and political parties, political views, health, and sexual life, and other personal information that may significantly infringe the privacy of the data subject. In addition, genetic information obtained through genetic testing, data of criminal record, personal physical, physiological, and behavioural characteristics, the information generated through certain technical means to identify a specific individual, and information on race or ethnicity are classified as sensitive information (Article23).

- The term “Personally Identifiable Information” means identification information assigned to distinguish an individual such as (a) resident registration number, (b) passport number, (c) driver's licence number, and (d) foreigner's registration number Article24).

2. Credit Information Use and Protection Act

- The term "credit information" means information prescribed by Presidential Decree, which is necessary to determine the creditworthiness of the other party to financial transactions and other commercial transactions, as follows: (a) Information by which a particular owner of credit information can be identified; (b) Information by which the transaction details of an owner of credit information can be determined; (c) Information by which the creditworthiness of an owner of credit information can be determined; (d) Information by which the credit transaction capacity of an owner of credit information can be determined; (e) Other information similar to that referred to in items (a) through (d) (Article2 No.1).

- "Personal Credit Information" is credit information of all individuals except for information on companies and corporations, and (a) information that can identify a specific individual through the name, resident registration number, and video of the information, (b) Information that makes it easy to recognize a specific individual by combining it with other information even if the information alone cannot recognize a specific individual (Article 2, No. 2).

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

- The pseudonym information in the Personal Information Protection Act means the pseudonymised information that is incapable of identifying a particular individual without the use or combination of information for restoration to the original state (Article2 No.1). The term “pseudonymisation” means a procedure to process personal information so that the information cannot identify a particular individual without additional information, by

deleting in part, or replacing in whole or in part, such information (Article2 No.1 (2)).

- A personal information controller may process pseudonymised information without the consent of data subjects for statistical purposes, scientific research, and preservation of records for the public interest, etc. (Article28 No.2 (1)). The Pseudonymous Data held by different companies can be combined by a specialised institution equipped with security facilities and can be released with the approval from the head of the specialised institution (Article28 No.3).

- The term "anonymous information" means the information that no longer identifies a certain individual when combined with other information, reasonably considering time, cost, technology, etc. the Personal Information Protection Act does not apply to such information (Article58 No.2).

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

The Act on Reporting and Using Specified Financial Transaction Information (Teuk Keum Bup), revised in March 2021, is the first law in Korea that deals with virtual asset transactions and virtual asset business operators, regulating illegal transactions or money laundering using virtual assets.

In the revised Act on Reporting and Using Specified Financial Transaction Information, the term "virtual asset" means an electronic certificate of economic value that can be transacted or transferred electronically (Article 2, No. 3). "Virtual asset business operator" means a person who runs a business of selling, purchasing, exchanging, transferring, and brokering, arranging, or acting, and storing and managing virtual assets (Article 2, No. 1).

- Obligation to report as a virtual asset business operator.

  Virtual asset business operators must report to the Financial Intelligence Unit (FIU), obtain ISMS certification from the Korea Internet & Security Agency, and submit a list of virtual assets it handles (Article 7 No.1). Both domestic and overseas operators are obligated to report.

- Obligation to secure a real-name account.

  Virtual asset business operators must secure real-name accounts and conduct financial transactions through the accounts that allow financial transactions between only the virtual asset business operator’s accounts and customer accounts.

- Anti-money laundering obligation.

  Virtual asset business operators must fulfil their obligations to prevent money laundering, such as customer verification, reporting suspicious transactions or high-value cash transactions (Article5 No.2). Particularly, in principle, virtual asset business operators cannot broker the sale and exchange of virtual assets between their customers and the customers of other virtual asset business operators. Exceptionally, virtual asset business

operators who fulfil their anti-money laundering obligations through licensing at home or abroad can broker only if they can check information about customers of the other virtual asset business operators who have traded with their customers (Article10 No. 20 of the Enforcement Decree). In addition, virtual assets with built-in technologies that make transfer records unidentifiable, such as dark coins and privacy coins, are prohibited (Article 28).

However, although the revised Act on Reporting and Using Specified Financial Transaction Information does not fall under the Personal Information Protection Act, the Personal Information Protection Commission recognises that there is a conflict with the Personal Information Protection Act due to the nature of blockchain technology and has applied a regulatory sandbox (deferral of personal information protection regulations) concerning the method of destroying personal information recorded on the blockchain.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

The revised Personal Information Protection Act, in effect since August 2020, introduced the concept of anonymous and pseudonym information, and in relation to this, the Personal Information Protection Committee enacted a notification in October 2021 on the combination and export of pseudonym information.

The notification on the combination and export of pseudonym information stipulates the combination procedure and method of pseudonym information, designation, and cancellation of the specialised institute, the criteria, and procedure for export and approval. Accordingly, the personal information controller can apply for the combination of pseudonym information to the specialised combination institute and take out the combined pseudonym information with the approval of the specialised combination institute.

The term "combination key" in the notification on the combination and export of pseudonym information means the information that is part of the pseudonym information that is the subject to the combination, that alone cannot recognise a specific individual but has been processed to be distinguishable from other information subject to the combination. The term "combination key linkage information" refers to information in which combination keys of different combination applicants are linked so that the combination keys may combine the same information. The term "combination key management agency" means the Korea Internet & Security Agency, which generates the combination key linkage information and provides it to a specialised combination institution.

The procedure for combining specific pseudonym information is as follows:

1. The combination applicant sends the combination key and serial number to the combination key management agency, and the combination target

information and serial number to the specialised combination agency, respectively.

2. The combined key management agency generates combined key linkage information from the information provided by the combination applicant and provides it to the specialised combination institute.

3. The specialised combination institute receives combination key linkage information from the combination key management agency, and combines the combination target information, and destroys the combination key linkage information.

However, notifications on the combination and export of pseudonym information are not directly related to blockchain-based applications or structures.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

If the personal information controller collects personal information, the following information can be used only for the purpose of the collection with the consent of the data subject (Article15).

1. The purpose of the collection and use of personal information.

2. Particulars of personal information to be collected.

3. The period for retaining and using personal information.

4. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

Korea's Personal Information Protection Act distinguishes and classifies the cases of transferring to or jointly using personal information with a third party as "providing to a third party" and "consignment". In the case of "providing to a third party", personal information is transferred to handle the third party's business and for the benefit of the third party, but "consignment" differs since the personal information is transferred to a third party to handle the personal information controller's business.

A personal information controller must inform a data subject of the following sections, and obtain consent from the data subject to provide the personal information to a third party overseas (Article17 No. 3).

1. The recipient of personal information.

2. The purpose for which the recipient of personal information uses such information.

3. Particulars of personal information to be provided.

4. The period during which the recipient retains and uses personal information.

5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

A personal information controller must disclose the details of the outsourced work and the entity that processes personal information under an outsourcing contract on the website of the personal information controller (Article26 No.2).

1. Contents of the entrusted work.
2. A person who is entrusted with and processes personal information processing (hereinafter referred to as a "trustee").

Meanwhile, Korea's Personal Information Protection Act provides special provisions for a personal information controller who is an information and communication service provider.

When an information and communication service provider provides, processes, or stores personal information overseas, the following contents must be notified to users, and consent must be obtained in accordance with special cases under the Personal Information Protection Act (Article 39 No.12).

1. Particulars of the personal information to be transferred.
2. The country to which the personal information is transferred, transfer date, and method.
3. Name of the person to whom the personal information is transferred (referring to the name of a corporation and the contact information of the person responsible for the management of information if the person is a corporation).
4. The purpose of using personal information by the entity to which the information is transferred and the period of retaining and using personal information.

10. Is it necessary to notify processing activities to any authorities?

Personal information controllers do not need to report personal information processing activities to the Personal Information Protection Committee. However, in all processes of collecting and using personal information, providing it to a third party, and consignment, all necessary measures such as explicit prior consent must be taken from the data subject as prescribed by the Personal Information Protection Act.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

Under the Personal Information Protection Act, the data subject reserves the following rights.

1. The right to be provided with information on the processing of personal information. The personal information controller must disclose matters

related to the processing of personal information, such as personal information processing policies, to the data subject and guarantee the rights of the data subject such as the right to request for inspection.

2. The right to select and decide whether to agree on the processing of personal information, the scope of consent, etc.

3. The right to check whether personal information is processed and request access to personal information.

4. The right to request the correction, deletion, and destruction of personal information. The personal information controller must take necessary measures, such as correction or deletion of personal information. However, if personal information must be collected according to other laws and regulations, deletion cannot be requested.

5. The right to request suspension of processing of personal information. The personal information controller must stop processing personal information without delay. However, there are cases where the request for suspension of processing of personal information by the data subject may be rejected, such as when there are special provisions in the law or when it is inevitable to comply with legal obligations.

6. Right to receive relief for damage caused by the processing of personal information promptly and fairly.

Korea's Personal Information Protection Act stipulates the right to request the correction, deletion, destruction, and suspension of processing of personal information, and the right to receive relief for damage caused by the processing of personal information and recognises the data subject's right to self-determination and damage relief concerning the right to be forgotten.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

The Personal Information Protection Act applies to anyone who is a personal information controller. However, there are no explicit legal interpretations or guidelines yet regarding whether individual nodes participating in the network of public blockchains or developers of public blockchain are personal information controllers.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The Personal Information Protection Act applies equally to public and private blockchains. In the case of the private permission blockchain, the network operator can be viewed as a personal information controller because there is a subject who designs and manages the blockchain, but there is no clear judgement or guideline on whether all individual nodes participating in the network are personal information controllers yet.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

- Modification and deletion of personal information

  The Personal Information Protection Act guarantees the right of the data subject to request the personal information controller to modify and delete personal information (Article 36). To modify or delete data stored in the blockchain, all participants in the blockchain can agree to proceed with the fork. However, in cases where a large number of anonymous participants are involved, such as public blockchains, it would be difficult to guarantee the rights of data subjects because it is practically impossible to secure such agreements whenever the data needs to be modified or deleted.

- Destruction of personal information

  The Personal Information Protection Act imposes an obligation on personal information controllers to destroy the collected personal information when the personal information becomes unnecessary due to the expiry of the retention period, attainment of the purpose of processing the personal information, or termination of transactions, etc. (Article 37).

  However, data stored in the public blockchain cannot be destroyed and is stored permanently, making it impossible for the personal information controller to fulfil its obligation to destroy.

- Consent to the collection, use, and provision of personal information

  The Personal Information Protection Act stipulates that the personal information controller's collection, use, and provision of personal information to a third party are possible only with the prior consent of the data subject (Article15, 17 No.2). Therefore, the personal information controller must obtain consent from all members for the collection and use of personal information for each node participating in the blockchain network. However, it seems practically impossible to obtain consent for each transfer to all anonymous participants who participated in the public blockchain.

- Liability for damages

  The Personal Information Protection Act stipulates that if a data subject suffers damage due to alteration or leakage of personal information, he or she can claim compensation for it (Article 39). However, in the blockchain environment, the object for damage claims is unclear, so there is a limitation to exercising the rights of the data subject. In the case of a public blockchain organised with a large number of anonymous participants, it would be difficult to identify the responsible party.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

There is no legal interpretation or guideline yet on how Korea's Personal Information Protection Act will be interpreted and applied to public and private blockchains.

However, concerning personal information destruction, the authorities have recently applied a regulatory sandbox that recognises the method of dividing the blockchain service into on-chain and off-chain, storing personal information off-chain and only hash values linked to actual data on-chain, and destroying personal information off-chain after achieving the purpose of processing personal information as deletion of personal information.

The Korea Centers for Disease Control and Prevention has established and operated a blockchain-based electronic vaccination certificate verification system in the issuance of the electronic COVID-19 vaccination certificate.

The blockchain node directly operated by the Korea Centers for Disease Control and Prevention records only the public key necessary to verify the authenticity of the electronic vaccination certificate and stores unique identification information of individual users such as resident registration numbers only on their smartphone.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

The Act on Reporting and Using Specified Financial Transaction Information, revised in March 2021, introduced a travel rule that requires virtual asset business operators to provide relevant information to virtual asset recipients when transferring virtual assets (Article6 No.3 of The Act on Reporting and Using Specified Financial Transaction Information).

The travel rule is applied to more than 1 million KRW, and the travel rule is applied only when transactions are made between virtual asset business operators (Article10 No. 10 of the Enforcement Decree). Therefore, if a customer transfers virtual assets worth more than 1 million KRW through a virtual asset business operator, the virtual asset business operator who transfers virtual assets is obligated to provide the following information to the virtual asset business operator who receives the virtual asset.

- Names of customers sending virtual assets and customers receiving virtual assets.
- Virtual asset addresses of customers sending virtual assets and customers receiving virtual assets.

Switzerland

Authors

Carmen De la Cruz Böhringer, LEXcellence AG

Ella Schröder, Lisk Foundation

The new Swiss Data Protection Act (DPA) has been finalised in September 2020 and will come into force in 2022. The act has been totally revised, but the core principles will naturally remain the same.

The biggest changes include the requirement to maintain records of data processing activities, obligation to report data losses and other data security breaches and the obligation to carry out data protection impact assessments. How these changes might impact the blockchain industry is examined closer in the sections below.

1. What are the legal acts regulating data privacy in your jurisdiction?

The main regulation for data privacy in Switzerland are:

- Federal Act on Data Protection (FADP)[84].
- Ordinance to the Federal Act on Data Protection (SR 235.11)[85].

Additionally there are provisions in several individual regulations.

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

- Federal Data Protection and Information Commissioner (FDPIC)[86].
- The cantons additionally have a data protection officer[87].
- Federal and cantonal Data Protection Offices as well as the corresponding courts.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

No.

But the government wants to further improve the framework conditions for companies in the area of blockchain and distributed ledger technology (DLT)[88]. On 14 December, 2018, it published a report on the legal framework for blockchain/DLT in the financial sector. The report shows that Switzerland's legal

[84] https://www.admin.ch/opc/en/classified-compilation/19920153/index.html. Note: the FADP is currently in parliament for a comprehensive revision. Entry into force is not expected before mid 2021.
[85] https://www.admin.ch/opc/en/classified-compilation/19930159/index.html.
[86] https://www.edoeb.admin.ch/edoeb/en/home.html.
[87] https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/schweiz.html.
[88] https://www.efd.admin.ch/efd/en/home/themen/Digitalisierung/blockchain.html.

framework is well suited to dealing with new technologies, including blockchain. Nevertheless, there is still a need for selective adjustments. Furthermore, the Federal Government has prepared a draft law on framework conditions for DLT/blockchain.[89] The draft law has not yet been discussed in Parliament.

The Federal Council proposes the following adjustments in particular:

- In the Swiss Code of Obligations, the possibility of an electronic registration of rights that can guarantee the functions of negotiable securities is to be created. This is intended to increase legal certainty in the transfer of DLT-based assets.
- In the Federal Law on Debt Collection and Bankruptcy, the segregation of crypto-based assets in the event of bankruptcy is to be expressly regulated, also to increase legal certainty.
- In financial market infrastructure law, a new authorisation category for so-called "DLT trading facilities" is to be created. These are intended to be able to offer regulated financial market players and private customers services in the areas of trading, clearing, settlement and custody with DLT-based assets.
- Finally, it should also be possible in future to obtain a licence to operate an organised trading facility as a securities firm. This requires an adaptation of the future Financial Institutions Act.

The adaptation of federal law will now be discussed by the parliament.

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

Current:

- "Data subjects" are natural or legal persons whose data is processed;
- "Controller of the data file" means private persons or federal bodies that decide on the purpose and content of a data file;
- "Processor" is undefined;
- "Federal Bodies" means federal authorities and services as well as persons who are entrusted with federal public tasks.

After revision of FADP (wording not yet final as of May 2020):

- "Data subjects" are natural persons whose data is processed;
- "Controller of the data file" is the federal body or private person who, alone or together with others, decides on the purpose, means and scope of processing;
- "Processor" means the federal body or private person who processes

[89] https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-77252.htm.

personal data on behalf of the controller.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Currently:

- Personal data is all information relating to an identified or identifiable person.
- Sensitive personal data includes data pertaining to:
    - religious, ideological, political or trade union-related views or activities,
    - health, the intimate sphere or the racial origin,
    - social security measures,
    - administrative or criminal proceedings and sanctions.
- Personality profile: a collection of data that permits an assessment of essential characteristics of the personality of a natural person.

After revision of FADP (wording not yet final as of May 2020):

- Personal data is all information relating to an identified or identifiable person.
- Sensitive personal data includes data pertaining to:
    - data on religious, ideological, political or other trade union views or activities,
    - data concerning health, privacy or racial or ethnic origin,
    - genetic data,
    - biometric data which uniquely identify a natural person,
    - data on administrative or criminal prosecutions and sanctions,
    - data on social assistance measures
- Profiling: (highly controversial and still under discussion in Parliament as of May 2020).

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

No, there is no definition in the regulation.

Generally speaking, it can be said that anonymisation of personal data is achieved if the person can no longer be identified.

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

For cryptocurrencies, there are money laundry and financial market legislations applicable. Other specific legislation, except data protection legislation, is not known.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

No, these have not been addressed.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

There is no general requirement to locally store the personal data. However, in some areas there may be specific requirements to be followed if it comes to cross-border transfer. For example, article 6 of the FADP that states the following:

Article 6 – CrossBorder Disclosure:

1. "Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.
2. In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if:
    a. Sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;
    b. The data subject has consented in the specific case;
    c. The processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;
    d. Disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
    e. Disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject;
    f. The data subject has made the data generally accessible and has not expressly prohibited its processing;
    g. Disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection

rules that ensure an adequate level of protection.

3. The Federal Data Protection and Information Commissioner (the Commissioner, article 26) must be informed of the safeguards under paragraph 2, letter A, and the data protection rules under paragraph 2, letter G. The Federal Council regulates the details of this duty to provide information."

10. Is it necessary to notify processing activities to any authorities?

As of today, there may be a duty to notify in some cases.

- See above, article 6 paragraph 3 (cross-country transfer).
- Federal bodies must declare all their data files to the Commissioner in order to have them registered.
- Private persons must declare their data files if:
    - They regularly process sensitive personal data or personality profiles; or
    - They regularly disclose personal data to third parties.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

The data subject has the following rights (article 6 FADP):

- Right of Information about available data concerning the subject, source of the data, purpose, legal basis, categories of the personal data processed, other parties involved, data recipient;
- Right that incorrect data will be corrected;
- Right of deletion of personal data;
- Right to block the release of personal data;
- Right to issue and transmit data (with revision).

There is currently no "right to be forgotten" in Switzerland (see comments on the pending changes to the Swiss Data Protection Act).

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

To date, there is no indication given to regulate these topics. The current and future Swiss Data Protection Act will apply.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

As long as there is personal data involved, it applies to both/all types of blockchain.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

The actions "use", "transfer" and "storage" all qualify as processing. If the data is considered personal data, all data protection laws apply.

On a public blockchain, the transaction history is always openly available. The users are not deemed to be anonymous, since their identity is concealed behind a pseudonym, the so-called public key or the wallet address. E.g., because it is possible to link a Bitcoin address from sender to recipient with the IP address, anonymity is not guaranteed. The identity is also disclosed when using wallet providers. Therefore, anonymity is not granted in blockchain transactions and personal data is processed within the meaning of Art. 3 let. a FADP applies. This will not change with the revised FADP either.

According to Swiss data protection law, every processor must adhere to the processing principles (Art. 4 FADP), ensure the accuracy of personal data (Art. 5 FADP) and provide sufficient data security (Art. 7 FADP). As data on a public blockchain is unchangeable, the data subject cannot request that incorrect data be corrected (Art. 5 Para. 2 FADP). Furthermore, data security is mainly guaranteed through the consensus mechanisms of the blockchain, which could be manipulated, e.g., bitcoin-miners with 51 % of the mining power can decide to change the blockchain in a certain way, therefore breaching data security. In order to comply with the privacy by design requirements security on the blockchain itself must be integrated in the solution as well.

Due to the nature of a public blockchain that whatever kind of (personal) data is stored in the block chain cannot be changed any more, the requirements of data subjects rights such as rectification rights or right of deletion of personal data cannot be guaranteed directly without further measures including but not limited to the structure of the blockchain solutions.

Compliance with FADP is therefore not possible if no further measures are put in place. A public blockchain solution may have to minimise the storage of personal data by design (security & data protection layers outside the blockchain), implement corresponding smart contracts etc. As each participant of a blockchain solution is controller and processor at the same time, these principles must be made transparent.

The issues as described will increase with the revised FADP: Data subject rights will be expanded and put inline with the EU General Data Protection Regulation (GDPR). Therefore the right to be forgotten, the right to request rectification of personal data etc. will be implemented which increases the clash with blockchain technology if no further measures are put in place. As the revised FADP has put in place a penal fine regime up to CHF 250'000 addressing every natural person

having violated data security requirements and further legal requirements (art. 61 revFADP), the pressure to check on the data protection requirements increases.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

In the absence of official recommendations, the processing of personal data should always follow a few main principles, such as data minimisation, purpose limitation and in Switzerland the widely used principle of acting in "good faith".

A few good practices would include on-chain and off-chain processing of data – this means that all the data that is not necessary to store on the blockchain should be kept off-chain. Although Switzerland is known for being a blockchain favourable country, there are still unclarities, which are most easily avoided by not storing all the data on the blockchain.

However, practices such as de-identification and pseudonymisation are also widely used, such as encryption. The decryption key is to be stored off-chain.

In the absence of official recommendations, the Swiss Federal Data protection and Information Commissioner (FDPIC) can also be contacted directly.

Another way to proceed in case no official recommendations in Switzerland can be found, is to follow the rules within the EU, since the EU interpretations strongly affect Swiss data protection as well.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

Under Swiss AML Legislation, VASPs are considered financial intermediaries. The travel rule has been established in Switzerland since August 2019.

Art. 10 of the Anti-Money Laundering Ordinance of the Swiss Regulator FINMA (hereinafter "AMLO-FINMA") states that financial intermediaries that process payment orders with other financial intermediaries must "...disclose the client's name, account number and address as well as the name and account number of the beneficiary. If no account number is available, the institution shall provide a transaction-referenced identification number. The address may be replaced with the client's date of birth and place of birth, his/her client number or his/her national ID number."

With this clause, FINMA has established more far-reaching rules for VASPs than the FATF. Unlike FATF, FINMA does not make an exception for the travel rule for payments involving wallets that are not hosted by another VASP. Therefore, even for transmissions to or from a wallet that is not supervised by a VASP ("external wallet"), the travel rule is applicable. The VASP must identify the beneficial owner

of the external private wallet or address, in the same manner as they would prior to engaging in any VA transaction with a client. This means that:

- The transaction to or from an external wallet of an existing client, the VASP must verify that the client has the power of disposal over the assets in the external wallet by "suitable technical means".
- The transaction to or from an external wallet of an external third party, the VASP must identify the third party, establish the beneficial owner and verify the power of disposal over the assets in the external wallets by using "suitable technical means".

Ukraine

Author

Vlad Nekrutenko, Legal Nodes

The research on the impact of personal data protection legislation on blockchain technology in Ukraine.

Done by Legal Nodes (https://legalnodes.com/).

1. What are the legal acts regulating data privacy in your jurisdiction?

- CoE's Convention 108 for the protection of individuals with regard to the processing of personal data
- Constitution of Ukraine (Art. 32): https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
- Law of Ukraine "On Protection of Personal Data" №2297-VI of 2010: https://zakon.rada.gov.ua/laws/show/2297-17
- Law of Ukraine "On Information" №2657-XII of 1992: https://zakon.rada.gov.ua/laws/show/2657-12
- Law of Ukraine "On Information Protection in Information Telecommunication Systems" №80/94-BP of 1994: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
- Law of Ukraine "On the Access to Public Information" №2939-VI of 2011: https://zakon.rada.gov.ua/laws/show/2939-17

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

Art. 22 of the Law of Ukraine "On Protection of Personal Data":

The competent authority is the Ukrainian Parliament Commissioner for Human Rights (Ombudsperson).

The Ombudsperson's role is being criticised due to the lack of effective enforcement instruments, as well as its dependence from the Ukrainian Parliament.

Until 2014, there was a State Service for personal data protection, which was liquidated due to the lack of independence.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

No specific blockchain-related regulation, guidance or opinions have been issued as of the time of this writing.

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

Art. 2 of the Law of Ukraine "On Protection of Personal Data":

- Personal Data Subject – an individual whose personal data is processed;
- Personal Data Controller – a natural or legal person who determines the purpose of personal data processing, establishes the scope of these data and the procedures for their processing, unless otherwise provided by law;
- Personal Data Processor – a natural or legal person to whom the personal data controller or the law gives the right to process this data on behalf of the controller;
- Recipient – a natural or legal person to whom personal data is provided, including a third party;
- Third Party – any person to whom the personal data controller or processor transfers personal data, except for the personal data subject, the personal data controller or processor and the Commissioner of the Ukrainian Parliament Commissioner for Human Rights.

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Art. 2 of the Law of Ukraine "On Protection of Personal Data":

Personal Data – information or a set of information about an individual who is identified or can be specifically identified;

Art. 11 of the Law of Ukraine "On Information":

Confidential Information about the individual – information that can be disclosed only upon the instruction of the data subject. Personal data concerning the exercise of official powers by an individual authorised to perform the functions of the state or local government are not confidential information.

Art. 7 of the Law of Ukraine "On Protection of Personal Data":

Special categories of personal data. The processing of personal data concerning racial or ethnic origin, political, religious or ideological beliefs, membership in political parties and trade unions, criminal liability records, and data relating to health, sexual life, biometric or genetic data is prohibited.

In accordance with Art. 9 of the Law of Ukraine “On Protection of Personal Data”, categories of personal data, processing of which requires the notification to the regulatory body (Ombudsperson), along with special categories defined in Art. 7, also include the information about administrative offences, the information about committing certain types of violence against a person, location and / or means of transportation of the person, application of pre-trial investigation measures to a person, and taking measures against the individual provided by the Law of Ukraine "On operational and investigative activities".

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

Art. 2 of the Law of Ukraine “On Protection of Personal Data”:

Depersonalisation of personal data – the removal of information that allows you to directly or indirectly identify a person.

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

No specific legislation was issued to date.

The current version of AML Law addresses the virtual assets providers as subjects of financial monitoring. However, nothing similar in the field of personal data protection was issued to date.

A number of draft legislative initiatives were developed. One of the examples is Draft law No.7485 of January 15, 2018 ‘On digital economy development’.

http://www.fst-ua.info/wp-content/uploads/2019/01/Cryptocurrency_Paper_Sept2018_en.pdf

https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110

None of the initiatives were signed into law to date.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

N/A.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

Generally, there is no data localisation requirement regarding the personal data in Ukraine.

However, there is a specific requirement for the processing of State information resources or information with limited access, the protection of which is established by law. In accordance with Art. 8 of the Law of Ukraine “On Information Protection in Information Telecommunication Systems”:

State information resources or information with limited access, the protection of which is established by law, must be processed in the system using a comprehensive system of information protection with confirmed compliance. Confirmation of conformity is carried out according to the results of the state examination as provided by the legislation. The result of the examinations is confirmed by the certificate of compliance.

To date, there is no certification procedure for foreign entities. This implies that the transfer of state-controlled personal data to third countries is barely possible.

In accordance with Art. 29 of the Law of Ukraine "On Protection of Personal Data", International transfers are allowed upon one of the following conditions:

- The country of the recipient provides adequate personal data protection. The following countries are considered adequate under Art. 29 of the Law on personal data protection: the EEA Member States, Parties to the Convention 108. The Cabinet of Ministers of Ukraine may provide a list of countries with adequate protection.

  [No list was issued as of the time of this writing];

- One of the following applies to the transfer:

  1. Personal data subject gave the consent to the transfer;
  2. The transfer is necessary for concluding the transaction for the benefit of the personal data subject;
  3. The transfer is necessary for the protection of vital interests of the personal data subject;
  4. The transfer is necessary for the public interest, the establishment, performance and ensuring legal claim;
  5. The personal data controller provides respective guarantees of non-intrusion in the private and family life of the personal data subject. [The scope and definitions of "respective guarantees are not defined or further provided in any Ukrainian act"].

10. Is it necessary to notify processing activities to any authorities?

In accordance with Art. 9 of the Law of Ukraine "On Protection of Personal Data", it is required to notify the Commissioner (Ombudsperson) on the processing activities that constitute a special risk to rights and freedoms of personal data subjects.

The processing of the following data categories requires the notification:

- racial, ethnic and national origin;
- political, religious or ideological beliefs;

- membership in political parties and / or organisations, trade unions, religious organisations or in public organisations of ideological orientation;
- health status;
- sexual life;
- biometric data;
- genetic data;
- administrative or criminal liability records;
- application of pre-trial investigation measures against the person;
- taking measures against the individual provided by the Law of Ukraine "On operational and investigative activities";
- committing certain types of violence against the individual;
- location and / or means of movement of the individual.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

Art. 8 of the Law of Ukraine “On Protection of Personal Data” provides data subjects with the rights to:

1. know about the sources of collection, location of their personal data, the purpose of their processing, location or place of residence of the personal data controller or processor or give a respective order to provide this information to authorised persons, except as provided by law;
2. receive information on the conditions for granting access to personal data, in particular information on third parties to whom their personal data is transferred;
3. access to their personal data;
4. receive no later than thirty calendar days from the date of receipt of the request, except as provided by law, an answer as to whether their personal data are processed, as well as receive the content of such personal data;
5. make a reasoned request to the personal data controller with an objection to the processing of their personal data;
6. make a reasoned request to rectify or destroy their personal data by the personal data controller and processor if this data is processed illegally or the data is inaccurate;
7. protect their personal data from unlawful processing and accidental loss, destruction, damage due to intentional concealment, its non-provision or late provision, as well as to be protected against the provision of information

that is inaccurate or disgrace the honour, dignity and business reputation of the individual;

8. file a complaint with the Commissioner (Ombudsperson) or with the court about the processing of their personal data;
9. apply legal remedies in case of violation of the legislation on personal data protection;
10. make reservations regarding the restriction of processing of their personal data when giving the consent;
11. withdraw the consent to the processing of personal data;
12. know the mechanism (logic) of automated processing of personal data;
13. be protected against an automated decision that has legal consequences for them.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

No specific regulation regarding the blockchain actors is issued in Ukraine to date. As a part of general discussion regarding the application of personal data in distributed environment, one can infer the following distribution of processing role:

- Blockchain users (participants) will be regulated as personal data controllers or processors, depending on the particular use case;
- Developers and providers of dApps will be regulated as personal data controllers. For B2B apps, which implies the processing of personal data on behalf of other organisations, the role will be the personal data processor;
- Nodes, depending on the level of instructions provided under the particular blockchain protocol by blockchain users, will either be regulated as personal data controllers or processors;
- Miners will presumably be regulated as personal data processors.

Personal Data Controller obligations:

- To have one of the legal grounds provided in Art. 11 of the Law of Ukraine “On Protection of Personal Data”;
- To notify the Commissioner (Ombudsperson) on the processing of personal data, which poses a special risk to the rights and freedoms of personal data subjects, within thirty working days from the date of such processing;
- To comply with the data protection principles provided in Art. 6 of the Law of Ukraine “On Protection of Personal Data”;

- To comply with the data subject rights provided in Art. 8 of the Law of Ukraine "On Protection of Personal Data";
- To protect personal data from accidental loss or destruction, from illegal processing, including illegal destruction or access to personal data;
- To notify the personal data subject about the data processing, including about the transfer of personal data to third parties;
- To delete or destroy the personal data upon one of the conditions specified in Art. 15 of the Law of Ukraine "On Protection of Personal Data";
- For the processing of personal data that requires the notification to the Commissioner (Ombudperson), to create or designate a structural subdivision or a responsible person that organises the work related to the protection of personal data during their processing. The information about such a unit must be delivered to the Commissioner (Ombudsperson);
- To comply with international transfers requirements provided in Art. 29 of the Law of Ukraine "On Protection of Personal Data".

Personal Data Processors obligations:

- Personal data processor is only allowed to process personal data for the purpose and in the scope specified in the agreement with the personal data controller;
- To comply with the data protection principles provided in Art. 6 of the Law of Ukraine "On Protection of Personal Data";
- To delete or destroy the personal data received from the personal data controller upon the end of relationships with the controller;
- To protect personal data from accidental loss or destruction, from illegal processing, including illegal destruction or access to personal data;
- To destroy the personal data upon the request of the data subject if those personal data are processed unlawfully or are inaccurate;
- To rectify the personal data upon the reasoned request from the data subject;
- For the processing of personal data that requires the notification to the Commissioner (Ombudperson), to create or designate a structural subdivision or a responsible person that organises the work related to the protection of personal data during their processing. The information about such a unit must be delivered to the Commissioner (Ombudsperson);

Only a state- or commune-owned enterprise is entitled to process personal data on behalf of the state or local authority bodies;

+ Art. 8 of the Law of Ukraine "On Information Protection in Information Telecommunication Systems":

- State information resources or information with limited access, the protection of which is established by law, must be processed in the system using a comprehensive system of information protection with confirmed compliance. Confirmation of conformity is carried out according to the results of the state examination in the order established by the legislation. The result of the examinations is confirmed by the certificate of compliance.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

General personal data protection requirements apply to any processing activities, including the processing using private and permissioned blockchains.

For more detailed information on personal data protection requirements, please see the previous question.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

No specific rules, guidance, or recommendations were issued to date. For general requirements, see answers to the above questions.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

- Hashing and salting of identifiers;
- Minimisation of data stored on-chain;
- Encryption of personal data linked to blockchain.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

Yes:

LAW OF UKRAINE On Preventing and Counteracting to Legalization (Laundering) of the Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction

Article 11. Due diligence

1. Reporting entities, which are financial institutions, shall be prohibited to open and keep anonymous (numbered) accounts and establish correspondent relations with shell banks as well as with banks and other

financial institutions being non-residents which are known to maintain correspondent relations with shell banks.

2. A reporting entity shall be obliged to perform each measure within the due diligence. A scope of actions when performing each measure within the due diligence shall be determined by a reporting entity subject to risk profile of a customer, in particular the risk level, purpose of business relations, the amount of conducted transactions, the frequency or duration of business relations.

3. Due diligence shall be conducted in the following cases: ...conducting virtual assets financial transaction in the amount that equals or exceeds UAH30,000;

Article 14. Information accompanying money or virtual assets transfer

1. In case of initiating a transfer to abroad including using virtual assets in an amount less than UAH30,000, or an amount equivalent to the specified amount, including in foreign currency, and the absence of signs of the connection of such financial transaction with other financial transactions amounting to more than UAH30,000, such a transfer shall be accompanied at least by the following:

    a. information about a payer (transfer initiator):

        i. an individual (individual entrepreneur) – surname, name and patronymic (if any); number of his/her account, from which money are debited and, in the absence of account, a unique identification number of financial transaction;

        ii. a legal entity – full name, number of an account, from which money are debited and, in the absence of account, a unique identification number of financial transaction;

        iii. a trust or other similar legal arrangement – full name, number of an account from which money are debited and, in the absence of account, a unique identification number of financial transaction;

    b. information about money transfer recipient:

        i. an individual (individual entrepreneur) – surname, name and patronymic (if any), number of an account, to which money are credited and, in the absence of an account, a unique identification number of financial transaction;

        ii. a legal entity – full name, number of an account, to which money are credited and, in the absence of an account, a unique identification number of financial transaction;

        iii. a trust or other legal arrangement – full name, number of an account, to which money is credited and, in the absence of an

account, a unique identification number of a financial transaction.

iv. a reporting entity, which provides money transfer services to a payer (transfer initiator), may not verify a payer (transfer initiator) in accordance with part two of this Article, except when:

1. there is a suspicion that financial transaction or a totality of related financial transactions may be associated with ML/FT/PF;

2. a reporting entity, which provides money transfer services to a payer (transfer initiator), receives from a payer (transfer initiator) cash for conducting transfer or e-money for their exchange/non-cash repayments for the purpose of their further transfer.

United Kingdom

Author

Sam Mottahedan, Blockchain for Human Rights

Laura Scaife, Datultacy

1. What are the legal acts regulating data privacy in your jurisdiction?

- The United Kingdom General Data Protection Regulation, Retained Regulation (EU) 2016/679 regime (UK **GDPR**)[90];
- Data Protection Act 2018 (**DPA 2018**);
- The Privacy and Electronic Communications Regulations (PECR) 2003[91].

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

The following are responsible: the Information Commissioner's Office (ICO) and the UK Courts for civil and criminal claims.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

The ICO has not published specific guidance on blockchain. However, in its response to the ESAs' joint committee discussion paper on the use of big data by financial institutions, the ICO states that any automated processing of personal data that produces a significant effect on an individual needs to be treated specially under the GDPR, including new technologies such as blockchain.[92] Where high risks prove difficult to mitigate, prior consultation with a data protection authority will be required.

The ICO also issued a joint statement on Facebook's Libra, asking for information on which procedures the platform is going to implement to ensure it complies with the GDPR and data subject's rights.[93] The statement did not offer suggestions on how Libra can comply with data protection regulations.

The ICO has a number of initiatives that may apply to blockchain notably:

- a grants programme (which promotes and supports research and solutions

[90] "Retained by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419)".

[91] These regulations were amended in 2004, 2011, 2015, 2016 and 2018 (See: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/privacy-and-electronic-communications-regulations/). Provides specific privacy rights in relation to electronic communications such as marketing calls, cookies, traffic and location data. See https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/.

[92] https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2013820/esa-big-data-consultation-ico-response- 20170321.pdf.

[93] https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf.

focused on privacy and data protection, including key privacy challenges of new technologies such as blockchain);[94] [95]

- a regulatory sandbox scheme, a service developed by the ICO to support organisations who are creating products and services which utilise personal data in innovative and safe ways. Participants will have the opportunity to engage with the ICO's Sandbox team, to draw upon its advice on mitigating risks and embedding "data protection by design". The ICO named as its key area of focus in 2021 – 2022 to provide support to innovators working with "products which utilises distributed ledger technologies (for example, in digital currencies or smart contracts) and are willing to work with [the ICO] to examine the data protection challenges associated with these (e.g. complex data controllership issues, facilitating individual rights requests, jurisdictional issues)";[96]

- a Technology Strategy from 2018–2021 to produce reports and address emerging risks and opportunities arising from technology including blockchain technology.[97]

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

The UK GDPR and DPA 2018 have largely similar definitions. UK GDPR Definitions:

- "Data subject" means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law; the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

- "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

DPA 2018 definitions:

- "Data subject" means the identified or identifiable living individual to whom personal data relates.

[94] https://ico.org.uk/about-the-ico/what-we-do/grants-programme-2018/.
[95] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-launches-latest-phase-of-privacy-innovation-grants-programme/.
[96] https://ico.org.uk/for-organisations/regulatory-sandbox/our-key-areas-of-focus-for-the-regulatory-sandbox-2021-22/.
[97] https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf.

- "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to: (i) an identifier such as a name, an identification number, location data or an online identifier, or (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

- "Controller" refers to a person who would be a controller under the GDPR. Where personal data is processed only: (i) for purposes for which it is required by an enact- ment to be processed, and (ii) by means by which it is required by an enactment to be processed, the person on whom the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller. The government is subject to the UK GDPR and each government department is to be treated as a person separate from the other government departments.

- "Processor" means any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Both the UK GDPR and the DPA 2018 identify three sets of personal data.

UK GDPR definitions:

- "Personal data" means any information relating to an identified or identifiable natural person.

- "Sensitive personal data" means data revealing racial or ethnic origin, political opin- ions, religious or philosophical beliefs, or trade union membership. The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

- Personal data relating to criminal convictions and offences ("Criminal Conviction Data").

DPA 2018 definition:

- "Personal data" means any information relating to an identified or identifiable living individual.

- "Sensitive data" has the same meaning as in the UK GDPR.

- "Criminal conviction data" has the same meaning as in the UK GDPR.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

Anonymisation

UK data protection law does not specifically define anonymisation. There is no legal obligation to anonymise data under the DPA 1998, the UK GDPR or any other

relevant legislation in the UK. However, to the extent that data is anonymised it will not be subject to the UK GDPR and/or DPA 1998. Certain aspects of the Privacy and Electronic Communications Regulations 2003 (PECR), that relate to "information" rather than "personal data", may still apply however.[98]

The ICO considers that the meaning of anonymisation is clear from the UK GDPR's use of the term "anonymous information" at Recital 26: "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."[99]

The ICO has interpreted Recital 26 as providing the basis for a defining "anonymisation" as "the way in which you turn personal data into anonymous information, so that it then falls outside the scope of data protection law. You can consider data to be effectively anonymised when it:

- does not relate to an identified or identifiable individual; or
- is rendered anonymous in such a way that individuals are not (or are no longer) identifiable".

The ICO suggests applying a "motivated intruder" test for ensuring the adequacy of anonymisation of information and whether it meets the scope of the definition (i.e., "whether an intruder would be able to achieve identification if they were motivated to attempt it").

For the purposes of data protection law, applying anonymisation techniques to turn personal data into anonymous information counts as data processing that falls within the scope of the UK GDPR.[100]

Pseudonymisation

The ICO considers that a definition for pseudonymisation can be derived from Article 4(5) of the UK GDPR as follows: *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"*.[101]

The ICO's "Anonymisation Code of Conduct" (2012) also offers a simplified definition for pseudonymisation: "The process of distinguishing individuals in a

[98] See guidance on cookies, traffic data, location data and similar technologies: https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/traffic-data/.

[99] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/#pd5.

[100] See https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf.

[101] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/#pd5.

dataset by using a unique identifier which does not reveal their 'real world' identity".

In its recent draft of its proposed updated guidance on anonymisation and pseudonymisation, the ICO defines [p]seudonymisation "as a technique that replaces or removes information that identifies an individual". It suggests that the information removed that can be used to identify individuals must be kept separately and appropriate technical and organisational controls must be in place for pseudonymisation to be effective and for the technique to be within the scope of the ICO's definition.[102]

The ICO considers that the term "*de-identified personal data*" in data protection legislation refers to data that has been pseudonymised.[103]

The ICO considers that "[p]seudonymisation is effectively only a security measure. It does not change the status of the data as personal data. Recital 26 makes it clear that pseudonymised personal data remains personal data and within the scope of the UK GDPR.[104]

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

There is no blockchain specific legislation in the UK.

Non-governmental bodies have issued guidance on blockchain and its interaction with other legislations in the UK, which have been deployed by UK legal practitioners:

- A report published by The Law Society (the independent regulator for the UK solicitor profession) in collaboration with the Tech London Advocates' (TLA) Blockchain Legal and Regulatory Group, which sets out key issues for legal practitioners to be aware of when advising on distributed ledger technologies (DLT). The report, entitled "Blockchain: Legal and Regulatory Guidance" (September 2020), includes a list of key recommendations on the many aspects relating to DLT, including commercial application, data governance, intellectual property, data protection measures, dispute resolution.[105]

- The UK Jurisdiction Taskforce (**UKJT**) (a taskforce of the Law Society's LawTech Delivery Panel) published a legal statement on crypto-assets and smart contracts following a public consultation.[98]

The Statement sets out that:

- "Crypto-assets" should be treated as "property" under common law (they meet the test in *National Provincial Bank v. Ainsworth* [1965] AC 1175), even though they do not fit neatly within the existing conventional categories of

[102] https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf.
[103] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/#pd5.
[104] Ibid.
[105] https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-report.

"things in possession" or "things in action".

- Crypto-assets can, at least to some extent, be owned, transferred, assigned and securitised.
- "Smart contracts" are capable of satisfying the basic requirements of an English law contract (depending, as any arrangement does, upon the parties' words and conduct).

The Statement should be considered in the context of the decision of Robertson v. Persons Unknown (unreported), 16 July, 2019, (Commercial Court), which explored the legal status of cryptocurrencies in the UK. The Statement is not binding and the UK Law Commission will need to decide if it wishes to legislate on these points or codify them. With regards to the common law, it is not clear how it will be interpreted by the courts, given that it is not binding and there is no requirement for the courts to give it consideration (for example, it does not have the binding effect of a statutory code of practice).

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

Yes, the ICO has published an "Anonymisation: Code of Practice (2012)"[106], which is currently being updated to take into account the UK GDPR and DPA 2018. Draft versions of the first two chapters of the updated guidance, entitled "draft Anonymisation, Pseudonymisation and Privacy Enhancing Technologies (May 2021)" were published in November 2021.[107]

Both ICO guidance addresses possible anonymisation and or pseudonymisation techniques. The following passages in guidance provide an overview of key anonymisation and/or pseudonymisation techniques addressed by the ICO:

- The ICO Anonymisation Code of Practice (2012), "Appendix 2 – Some key anonymisation techniques" – sets out a list of anonymisation techniques.[108]
- The ICO Anonymisation Code of Practice (2012) "Annex 1" "Annex 2" and "Annex 3" – which shows how a set of personal data can be converted into various forms of anonymised data, using case-studies and practical examples.
- Chapter 2 of the draft Anonymisation, Pseudonymisation and Privacy Enhancing Technologies "guidance" – sets out tests for organisations to test the GDPR-compliance of anonymisation techniques.

The ICO advises that encryption and hashing are pseudonymisation techniques. Therefore, hashing and encryption would not be considered as an anonymisation

[106] https://ico.org.uk/media/1061/anonymisation-code.pdf.

[107] See https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/.

[108] https://ico.org.uk/media/1061/anonymisation-code.pdf.

technique, and the encrypted data is subject to the UK GDPR.[109]

In reality, the guidance makes it clear there is no one technique to anonymise and pseudonymise data. The ICO notes that "the risk of re-identification through data linkage is essentially unpredictable because it can never be assessed with certainty what data is already available or what data may be released in the future". The ICO therefore intends to provide flexibility to organisations, by advising a proportionate and risk-based approach on the possibility of re-identification of anonymised/pseudonymised data. The ICO notes that it will take advice in guidance into consideration where there is an issue about the effectiveness of anonymisation, and therefore that taking into account good practice recommendations in guidance will put organisations in good stead.[110]

Techniques and approaches that are designed to turn personal data into anonymous and/or pseudonymisation information constitute processing operations performed on that data. This means that organisations need to comply with data protection requirements for this processing and should consider the UK GDPR and DPA 2018. This includes ensuring the organisation has a lawful basis for it and clearly defines its purpose(s). The ICO notes that “[I]n general it is likely that applying anonymisation techniques to the personal data you hold will be fair and lawful. However, it is still necessary for you to clearly define your purpose and detail the technical and organisational measures you intend to implement to achieve it.” [111]

The UK courts have rarely considered anonymisation techniques. In 2011, in R (on the application of the Department of Health) v. Information Commissioner [2011] EWHC 1430 the UK High Court found that data about certain abortions had been successfully anonymised by being turned into statistical information. However, this case was decided under Data Protection Act 1998 (DPA 1998). From then, the article 26 Working Party took a “zero risk” approach to anonymisation stating that “anonymisation results from processing personal data in order to irreversibly prevent identification”, which is inconsistent with the findings in the High Court Case. In any event, turning data into statistical information is unlikely to be a helpful anonymisation method for blockchain based applications.

Pre-Brexit European guidance on anonymisation and pseudonymisation can also be used by organisations to understand likely interpretations of UK GDPR, particularly where the issue is not directly addressed in ICO guidance European Parliament published a study on blockchain and the GDPR, which summarises European regulators’ approach to the application of data protection regulation to blockchain technologies.[112] The study clarifies that hashing and encryption are not anonymisation techniques. The study identifies various pseudonymisation techniques, including homomorphic encryption, stealth addresses and the addition of “noise” to the data. In 2018, the European Parliament issued a report on blockchain in which zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARK) is highlighted as an innovation made to comply with data protection by design.[113] This, combined with other pseudonymisation techniques,

[109] https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf.
[110] https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf.
[111] Ibid.
[112] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.
[113] https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html.

could assist with reaching the anonymisation threshold under the GDPR.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

There is no requirement to store personal data locally. Any international transfers of personal data outside of the European Union and following the end of the transition period outside of the UK, need to be subject to appropriate safeguards, for example a finding of adequacy or an overseas data transfer mechanism such as Privacy Shield, Binding Corporate Rules or Standard Contractual Clauses.

10. Is it necessary to notify processing activities to any authorities?

Yes, any organisation or sole trader who processes personal data needs to register with the ICO and pay a data processing fee, unless exempt.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

Data subjects have the following rights:

- right to be informed;
- right of access;
- right to rectification;
- right to erasure;
- right to restrict processing;
- right to data portability;
- right to object to certain processing;
- rights in relation to automated decision making and profiling; and
- right to withdraw their consent to processing.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

Anyone processing personal data would be required to comply with the GDPR. Any participant in the blockchain who has the right to write on the chain or send data for validation to the miners will be categorised as a data controller for the purposes of the GDPR. If multiple participants carry out processing operations with a common purpose and a data controller for the processing is not identified beforehand, all participants involved in that processing will be considered joint data controllers.

Miners who only validate transactions on the chain will not be considered data controllers, but may be considered data processors if they follow the controller's

instructions when checking transactions.

Any natural person (i.e., individual) who enters personal data on the blockchain is not considered a data controller, provided that the processing of data does not relate to its professional or commercial activity.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The GDPR and DPA 2018 will apply to both private and permissioned blockchains to the extent they involve the processing of personal data (including storing and transferring).

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

The main data privacy challenges in the UK when using public blockchain are as follows:

Risks of data being classified as "personal data", even after applying anonymisation techniques: Where personal data has been pseudonymised (that is, could still identify an individual in conjunction with additional information), it is still classed as personal data. Encryption and hashing (commonly used on blockchain networks) are considered pseudonymisation techniques by the ICO and therefore still likely within the scope of the UK GDPR. Given the immutability of blockchain and the conflicts between UK GDPR and blockchain networks, ensuring that data is not classified as personal data remains a significant privacy challenge for public blockchains. While steps can be taken to mitigate risks of transactional data being classified as 'personal data' under the UK GDPR, there is at present no legal certainty for developers wishing to handle public keys in a GDPR compliant matter. The status of anonymity solutions such as Zero Knowledge Proofs (ZKP) have yet to be confirmed by the ICO.

Data Protection Impact Assessments: The UK GDPR mandates that controllers carry out a data protection impact assessment for operations that presents specific risks to individuals due to the nature or scope of the processing operation (Article 35(1) of the UK GDPR). It is unclear at the moment whether the use of a blockchain could automatically trigger an obligation to carry out a data protection impact assessment on controllers in the context of a blockchain network.

Privacy Notices: The UK GDPR requires controllers to provide data subjects with certain prescribed information – typically set out in a privacy notice – when the data is either collected directly from the individuals or is collected via a third party (Article 13 and Article 14, UK GDPR). This may be difficult in the blockchain context where the status of parties (controllers vs processors vs joint controllers) are unclear, and where parties are unable to identify a method to communicate privacy information to data subjects.

Lawful basis for processing: The UK GDPR mandates that processing can only be carried out in reliance of one of the lawful bases set out in Article 6. For special category data, organisations must also rely on an additional lawful basis as set out

in Article 9 and 10 of the UK GDPR. A particular difficulty is relying on consent as a lawful basis in the blockchain context. Consent under the UK GDPR must be capable of being withdrawn for it to be relied upon by organisations. Where personal data is being stored on an immutable blockchain, organisations that routinely rely on consent as a lawful basis for processing may find that they are unable to store personal data in a manner that is GDPR-compliant.

Storage of Data: Personal data under the UK GDPR must be kept in an identifiable form for no longer than necessary for the purposes for which it is processed (Article 5(1)(e), UK GDPR). This raises difficulties where personal data on-chain cannot be deleted. Organisations will need therefore to be able to justify any remaining personal data as being required for the duration of the blockchain. "Pruning" and "forking" are possible options, although these may contradict the benefits inhering to the immutability of public blockchain technology as well as be technologically expensive and difficult .

Individual Rights: Particular attention should be paid to the right to object (Article 21, UK GDPR), right to rectification (Article 5(1)(d), UK GDPR), and the right to restrict processing (Article 18, UK GDPR) given the apparent incompatibility of these rights with the immutable nature of many public blockchain networks. "Pruning" and "forking" are possible options, although these may contradict the benefits inhering to the immutability of public blockchain technology as well as be technologically expensive and difficult.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

There is currently no legal certainty or guidance for ensuring that personal data processed in both public and private blockchains is processed in a manner that is UK GDPR-compliant. Most best practices revolve around preventing transactional data being considered "personal data" under the UK GDPR in the first place to avoid conflicts with the UK GDPR inhering to blockchain networks.[114] For example, by keeping details of each party's identity off-chain to enable it to be modified and deleted or alternatively, by using a private, permissioned blockchain network with governance frameworks that enables erasure and modification of personal data.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

On 22 of July 2021, HM Treasury (UK Government's finance ministry) invited the public to provide views and evidence on its proposal to amend the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 to keep the UK compliant with FATF recommendations and

[114] For more examples, see https://www.lawsociety.org.uk/en/topics/research/blockchain-legal-and-regulatory-guidance-report.

implement its "travel-rules".[115]

In its consultation to the public, the HM Treasury proposed that crypto assets firms will need to put in place systems for ensuring that personal information of the originator and beneficiary of a crypto asset transfer is transmitted and received alongside the transfer, in an appropriate format.

The receiving crypto asset service provider will be required to retain the above beneficiary and originator information for a period of five years from the date it reasonably believes the transaction is complete. In order to protect the privacy of the parties to the transaction, this information must be deleted at the end of this five year period, unless Regulation 40 of the MLRs or a court ruling requires it to be held for longer (para 6.18 of the consultation document). Crypto asset service providers will be required to make this information available fully and without delay in response to a written request by the FCA, HMRC, the NCA or the police, where this information is reasonably required in connection with the authority's functions (para 6.19).[116]

The following information will be required on the originator of the transaction (para 6.11):

- Name
- Address
- Account number or unique transaction identifier.
- For transfers above 1,000 GPB, personal document number.
- For transfers above 1,000 GPB, customer identification number or date and place of birth.

The following information on the beneficiary of the transactions:

- Name
- Account number/unique transaction identifier.

HM Treasury is analysing the feedback and has committed to publishing a full review report by 26 June 2022, after which legislation could be introduced in Parliament.[117]

---

[115] https://www.gov.uk/government/consultations/amendments-to-the-money-laundering-terrorist-financing-and-transfer-of-funds-information-on-the-payer-regulations-2017-statutory-instrument-2022.

[116] Ibid.

[117] https://www.lawsociety.org.uk/campaigns/consultation-responses/amendments-to-the-money-laundering-regulations-2017-statutory-instrument-2022.

United States

Authors

Odia Kagan, Fox Rothschild

Caroline A. Morgan, Culhane Meadows

1. What are the legal acts regulating data privacy in your jurisdiction?

The US does not have a comprehensive data protection law. Instead, data protection is regulated by sector-specific laws. For example, the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191-Aug. 21, 1996, protects processing of personal health information by certain entities, the Gramm Leach Bliley Act (GLBA), 15 U.S.C. §§ 6801 et seq., and the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., govern the privacy of information for financial institutions and certain uses pertaining to credit reporting, and the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501 et seq., addresses the use by operators of commercial websites of personal information of children under 13.

In addition, many of the so called "unregulated entities" (those not regulated by sector-specific laws) are subject to the jurisdiction of the US Federal Trade Commission (FTC), the "de facto" privacy regulator that, for the past approximately 23 years has been adjudicating data privacy and information security issues pursuant to its authority under Section 5(a) of the FTC Act regarding unfair or deceptive acts or practices in or affecting commerce.

At the state level, there are 50 separate data breach notification laws. In addition, at least 25 states have laws addressing information security of private sector entities. A number of states including California, Delaware and Nevada have laws requiring privacy disclosure for personal data collected on a website. In January 2020, the California Consumer Privacy Act (CCPA) was passed: Cal. Civ. Code §§ 1798.100-1798.199. It is the first comprehensive data protection law in the US and governs the collection of personal information of California state residents. CCPA provides enhanced privacy rights relating to the access to, deletion and sharing of personal information collected by businesses.

In November 2020, California voters approved the California Privacy Rights Act (CPRA), commonly referred to as CCPA 2.0 because it amends and expands CCPA. It provides separate requirements and prohibitions concerning using sensitive personal information, provides new privacy rights like the right to correction and the right to opt out of automated decision making technology, expands existing rights and adopts GDPR-like principles such as: data minimisation, purpose limitation, storage limitation and data protection impact assessments (DPIA). It also establishes a dedicated data protection authority. Most of CPRA's provisions will not take effect until 1 January, 2023, but it does contain a look back period to January 1,2022 and businesses must comply with CCPA in the meantime.

In March 2021, the Virginia Consumer Data Protection Act ("VCDPA") was passed: Code of Virginia §§ 59.1-575 – 59.1-585. It is the second comprehensive data protection law in the US and concerns the collection of personal data of Virginia state residents. VCDPA provides Virginia residents the enhanced privacy rights CCPA provides and will go into effect on 1 January, 2023.

In July 2021 the Colorado Privacy Act ("CPA") was signed into law, with similar provisions to VCDPA and became the third comprehensive data privacy law in the US: Colorado Senate Bill 190. It goes into effect on July 1, 2023.

Personal information stored on the blockchain would be regulated: (i) under sector-specific laws (e.g., GLBA if used by a financial institution or HIPAA if used by a covered entity to process protected health information), (ii) under Section 5 of the FTC Act for unfair or deceptive acts or practices; (iii) under state-specific data breach or information security laws in the context of a data breach; or (iv) CCPA and CPRA (where pertaining to the residents of the state of California); or (v) VCDPA /CPA (where pertaining to the residents of the state of Virginia/ Colorado).

2. What authority(ies) are responsible for data protection and enforcing the data protection regulation(s)?

Entities that are subject to a sector-specific law are subject to the jurisdiction of the authority responsible for enforcement of such law. For example, for HIPAA it is the Department of Health and Human Services' Office for Civil Rights, whereas the Children Online Privacy Protection Rule (COPPA) is enforced by the Federal Trade Commission, and the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act are enforced by the Federal Trade Commission and/or the Consumer Financial Protection Bureau (CFPB).

The Federal Trade Commission has been the de facto privacy regulator for "unregulated entities".

State privacy laws are generally enforced by the state's Attorney General, with CPRA being enforced by the newly established California Privacy Protection Agency (CPPA).

Finally, in some instances state laws (for example, CCPA) provide a private right of action to seek damages through legal claims and class action lawsuits.

3. Have these authorities issued any specific regulations, guidance or opinions on blockchain? If yes, please summarise.

Regulation of the blockchain in the US has, to date, been carried out mostly in connection with the cryptocurrency and securities aspect with various agencies including the Department of Treasury, Securities and Exchange Commission, Federal Trade Commission, Internal Revenue Service, and Financial Crimes Enforcement Network, who all define "cryptocurrency" differently and have varying positions on how regulation should be applied. In addition to federal guidelines, states have also introduced their own rules and regulations. In 2015, New York was the first state to regulate virtual currency companies. Thirty-three states had pending legislation in the 2021 legislative session pertaining to

blockchain or cryptocurrency. As of 2019, 32 states have proposed legislation promoting distributed ledger technology.

In the context of data protection on the blockchain there have been a few guidance papers:

- The FTC created a Blockchain Working Group to study how blockchain technology can address consumer data privacy concerns by increasing consumers' control over information pertaining to them.
- Likewise, multiple states have created blockchain working groups. For example, in 2018, California enacted legislation requiring a blockchain working group to evaluate the risks, benefits and legal implications of blockchain, and to recommend amendments to current legislation that blockchain may impact. Moreover, the Attorney General of Vermont established a Blockchain Working Group to determine whether blockchain specific legislation is necessary to protect consumers. In June 2021, Congresswoman Maxine Waters, Chairwoman of the House Committee on Financial Services, announced that she organised a Digital Assets Working Group of Democratic Members that will consider how legislation can protect consumers in the digital asset and cryptocurrency space.

Following the appointment of former FTC Commissioner Rohit Chopra as director of the CFPB, many are speculating[118] the CFPB will take an expansive view of the bureau's authority and will take action against companies in the blockchain space (and specifically crypto companies) for "unfair, deceptive, or abusive acts or practices" prohibited by the Dodd-Frank Act. Chopra said at a hearing before the Senate Banking Committee that he intends to look closely at how technology giants including Facebook Inc. plan to use digital currencies as part of his wider probe into how the companies are harvesting and using consumer financial data. Challenges to the power of the CFPB will likely follow.

In addition, in August 2021, U.S. Senate Banking Committee Ranking Member Pat Toomey (R-Pa.) announced[119] he was soliciting ideas and legislative proposals to ensure federal law supports the development of emerging cryptocurrency and open blockchain network technologies while continuing to protect crypto investors. Proposals sought include privacy, due process, investor, and consumer protection.

4. What kind of actors (e.g., data subjects, controllers, processors…) does the applicable data protection regulation in your jurisdiction mention? Please provide legal definitions.

To the extent HIPAA applies, the relevant actors would be a covered entity or a business associate:

[118] https://www.americanbanker.com/news/push-to-regulate-crypto-could-test-limits-of-cfpbs-power.
[119] https://www.banking.senate.gov/newsroom/minority/toomey-requests-feedback-on-clarifying-laws-around-cryptocurrency-and-blockchain-technologies.

- A "covered entity" is (1) "a health care provider who transmits any healthcare information in electronic form in connection with [certain transactions covered by HIPAA]," (2) a health plan or (3) a health care clearinghouse.

- A "business associate" is a person who "(i) on behalf of such covered entity or of an organised health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains or transmits protected health information for a function or activity regulated by [HIPAA] or (ii) provides, other than in the capacity of a member of the workforce of such covered entity, legal actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for such covered entity, or to or for an organised healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person."

To the extent GLBA applies, the relevant actors would be financial institutions or service providers to them.

Under GLBA, a "financial institution" is any institution the business of which is engaging in activities that are financial in nature including:

- "Lending, exchanging, transferring, investing for others or safeguarding money or securities.

- Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability or death, or providing and issuing annuities, and acting as principal, agent or broker for purposes of the foregoing, in any State.

- Providing financial, investment, or economic advisory services, including advising an investment company.

- Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly.

- Underwriting, dealing in, or making a market in securities.

- Engaging in any activity that [has been determined] to be so closely related to banking or managing or controlling banks as to be a proper incident thereto.

- Engaging, in the United States, in any activity that a bank holding company may engage in outside of the United States [and [that has been determined] to be usual in connection with the transaction of banking or other financial operations abroad.

- Directly or indirectly acquiring or controlling, whether as principal, on behalf of one or more entities, or otherwise, shares, assets or ownership interests of a company or other entity, whether or not constituting control of such

company or entity, engaged in any activity not authorized pursuant to 12 U.S.C. § 1843 [in certain circumstances].

- Directly or indirectly acquiring or controlling, whether as principal, on behalf of one or more entities or otherwise, shares, assets, or ownership interests of a company or other entity, whether or not constitution control of such company or entity, engaged in any activity not authorized pursuant to 12 U.S.C. § 1843 [in certain circumstances.]"

A "Service Provider" is defined as "any party that is permitted access to a financial institution's customer information through the provision of services directly to the institution."

To the extent CCPA applies, the relevant actors would be: a "business," a "service provider" and a "third party."

- "Business" is defined as an entity that determines the purposes and means of processing a consumer's personal information.

- A "service provider" is an entity that "processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract. Though service providers are not permitted to sell personal information, they can use personal information internally "to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source[,]" which is broader than the definition of "data processor" under GDPR. Section 999.314(c)(3).

- A "third party" is "a person who is not any of the following: (1) [t]he business that collects personal information from consumers [] [,](2)[a] person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract[.]"

CPRA introduces another relevant actor, the "contractor," defined as a person to whom a business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business.

To the extent VDCPA or CPA applies, the relevant actors would be a "controller," a "processor," and a "third party":

- "Controller" is defined as "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."

- A "processor" is defined as "a natural or legal entity that processes personal data on behalf of a controller."

- A "third party" is "a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller."

5. How does the applicable data privacy regulation define personal data and does it provide for different categories of personal data?

Generally, state data breach laws broadly define personal information. For example, under New York State law, personal information is any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify the natural person. New York's statute further defines private information to include personal information in combination with certain data elements including a social security number, driver's licence number, biometric information, or a username or email address in combination with a password or security question and answer that would permit access to an online account. Private information is the only information that triggers a breach notification in New York.

Under GLBA, "nonpublic personal information" is (i) "personally identifiable financial information and: (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

Personally identifiable financial information meets the following criteria: (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."

Under HIPAA "protected health information" is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and

(i) information that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Under CCPA "personal information" is defined as "information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household." CCPA does not contain special categories of personal data, but it does state that personal information includes, but is not limited to, biometric information, professional or employment related information, education information, geolocation data, internet activity like browsing history or search history and identifiers like name, alias, postal address, among others. CCPA does not have a special category for sensitive personal information nor does it categorise sensitive data. CPRA on the other hand, provides for "sensitive personal information" which includes a consumer's social security, driver's license, state identification card or passport number, a consumer's precise geolocation, a consumer's racial or ethnic origin and personal information collected and analyzed concerning a consumer's health, sex life or sexual orientation, among others.

Under VDCPA "personal data" is defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person[,] [and] does not

include de-identified data or publicly available information." VDCPA also defines "sensitive data" which is "a category of personal data that includes: 1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; 2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person; 3. The personal data collected from a known child; or 4. Precise geolocation data." This is all similar in CPA other than the specific mention of precise geolocation data. VDCPA also defines "biometric data" as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual[, and] does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA. CPA does not have a parallel definition. Finally, VDCPA defines "precise geolocation data" to mean "information derived from technology, including but not limited to global positioning systems level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet[, and] does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility. CPA does not have a parallel definition.

6. Does the applicable data privacy regulation define anonymisation and/or pseudonymisation?

CCPA defines deidentification, aggregation and pseudonymisation. The definition of deidentification is different than its parallel "anonymisation" under GDPR as it also imposes policy/contractual requirements be fulfilled,

- "Deidentified" "[M]eans information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information [h]as implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain[,] [h]as implemented business processes that specifically prohibit reidentification of the information[,] [h]as implemented business processes to prevent inadvertent release of deidentified information[,] [and] [m]akes no attempt to reidentify the information."

- "Aggregate consumer information" "[M]eans information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. 'Aggregate consumer information' does not mean one or more individual consumer records that have been deidentified."

- "Pseudonymise" or "Pseudonymisation" "[M]eans the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organisational measures to ensure that the

personal information is not attributed to an identified or identifiable consumer."

As per the CPRA:

"Deidentified" "means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information takes reasonable measures to ensure that the information cannot be associated with a consumer or household, publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision, and contractually obligates any recipients of the information to comply with all provisions of this subdivision."

"Aggregate consumer information" has the same definition as CCPA.

"Pseudonymise" or "Pseudonymisation" has the same definition as CCPA.

VDCPA defines "de-identified data" and "pseudonymous data."

- "De-identified data" is "data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person."
- "Pseudonymous data" is "personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person."

CPA defines "de-identified data" as "any data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual or a device linked to such an individual if the controller that possesses the data" takes steps to ensure that it remains de-identified which are similar to those in CPRA (reasonable measures; public commitment, contractual obligations).

The CPA definition for pseudonymous data is similar to that of VCDPA.

7. Is there any specific legislation that impacts using blockchain technology in your jurisdiction? Does it refer to data privacy?

At least thirty-three states have pending legislation in the 2021 legislative session pertaining to blockchain or cryptocurrency. In 2019, 28 states introduced legislation relating to blockchain. Some states have enacted legislation that supports the use of blockchain technology largely in the digital assets or smart contract space. Delaware was the first state to enact legislation to allow businesses to use blockchain for corporate recordkeeping and other states have introduced similar bills. In addition, Colorado has enacted legislation that promotes the use of blockchain technology to protect confidential data in state records. Multiple states have created blockchain working groups or legislation requiring the studying of

blockchain, like North Dakota who passed legislation that requires its Department of Information Technologies to research and develop the use of blockchain for data transfer and storage, to improve internal data security and identify external hacking threats. In addition, for regulation and guidance on blockchain in the context of cryptocurrency see Section 3 re: "authorities issuing specific regulation, guidance or opinions on blockchain."

Otherwise, to the extent personal information is included in the blockchain venture, CCPA/CPRA, VDCPA and CPA would apply. As you can see above, the definition of personal data and personal information is broad, with the latter including online and electronic identifiers.

In addition, as mentioned above, the FTC and/or CFPB could regulate conduct involving personal information on the blockchain as misleading, unfair or deceptive conduct.

8. Have any particular anonymisation or pseudonymisation techniques been addressed by the data privacy authorities, courts or experts in your jurisdiction? Are they relevant for blockchain-based applications and architectures?

CCPA and CPRA include definitions of deidentification and pseudonymisation, while VDCPA /CPA defines "de-identified data" and "pseudonymous data" (see above). As CCPA is new and CPRA, VDCPA and CPA have not yet taken effect, this has not been tested in court.

Under HIPAA, PHI can be deidentified using the Expert Determination Method and the Safe Harbor Method. Under the Expert Determination Method, an expert examines data and determines an appropriate means to de-identify the data with a low likelihood of reidentification. Conversely, the Safe Harbor Method permits a covered entity to consider data as de-identified by removing 18 specific types of data including names, fax numbers, social security numbers, account numbers and internet protocol (IP) addresses, among others. There is currently an ongoing discussion about the discrepancy between the definition under CCPA and that under HIPAA including a proposed bill AB 713 that would amend CCPA to harmonise it with the de-identification standards in HIPAA.

Under GLBA, personally identifiable financial information does not include information that does not identify a consumer such as aggregate information or blind data that does not contain personal identifiers, such as account numbers, names or addresses.

The preeminent US standards entity, NIST, has published a guide on deidentification techniques and a draft guidance for de-identifying government data sets.

The CCPA/CPRA/VCDPA/CPA definitions of deidentified information requires that the information "cannot reasonably identify, relate to, describe, be capable of being associated with or be linked, directly or indirectly." In the absence of a guidance or implementation, enforcement/guidance under GDPR for anonymisation in connection with the blockchain may be applicable. For HIPAA or GLBA, the relevant definitions under such laws would need to be met.

9. Is there a requirement to store personal data locally and how do international transfers work in your jurisdiction?

Generally, and with few narrow exceptions, US data protection laws (including GLBA, HIPAA, CPRA and CCPA) do not restrict international data transfers nor require that processing be localised, and do not have a specific territorial scope with regard to where a business processes information. The important factor to consider is that you can meet all the legal requirements, including information security requirements, through your provider in the offshore jurisdiction.

10. Is it necessary to notify processing activities to any authorities?

In the data protection context (as distinguished from licensure requirements for blockchain in the context of cryptocurrency), there is no overarching registration requirement. However, if the blockchain operator is deemed to be a data broker, registration may be required under the laws of Vermont and California. Under Vermont law, a "data broker" is a business that collects and sells or licences to third parties the brokered personal information of a consumer that the business has no direct relationship with. Data brokers are required to register with the Vermont Secretary of State and maintain certain minimum data security standards. The purpose of this registration is to give consumers access to information to protect themselves against certain data broker activities. Under California law, if a data broker sells consumers' private information (as defined by the CCPA) it is required to register with the California Attorney General.

11. Can you describe what rights do data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?

Under CCPA, California residents have five rights with regard to personal information: (1) the right to know what categories of personal information ["PI"] have been collected and the purpose for the collection, (2) the right to access, including copies of PI, (3) the right to be forgotten, subject to some exceptions, (4) the right to opt-out of the sale of PI to third parties and (5) the right to exercise these rights without retaliation. CPRA expands on the above rights and adds new ones including chiefly: (1) the right to limit use of sensitive personal information, (2) the right to correct information, (3) expands CCPA's right to opt-out of third-party sales by including the right to opt-out of sharing of PI, (4) the right to access information about automated decision making and (5) the right to opt-out of automated decision making technology. Individuals have the right to appeal if a business does not take action on their requests.

VCDPA and CPA provide for similar rights but also specifically list out the right to data portability (obtain a copy in a portable and reading usable format that allows switching to another controller easily) and allow for a process of appealing a business' denial to act within a reasonable time.

Under HIPAA, an individual has (1) the right to ask to see or get a copy of their medical record or other health information, (2) the right to ask to change any wrong information in their file or add information to their file if they think

something is missing or incomplete, (3) the right to learn how their health information is used and share by your doctor or health insurer, (4) the right to let their health providers or health insurance companies know if there is information they do not want to share and (5) the right to ask to be reached by phone or mail somewhere other than their home.

Generally, under GLBA, a consumer has the right to receive a notice of a financial institution's privacy policies and practices with regard to affiliated and nonaffiliated third parties and the right to opt out of disclosure of their nonpublic personal information from a financial institution to a nonaffiliated third party if no exceptions apply permitting the disclosure.

12. Which actors in public blockchain networks would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

To the extent CCPA CCPA or the other US state privacy laws applies, the entity responsible would be the one that determines the purpose and means of processing, provided that it meets with the other criteria to render it subject to CCPA. See above for definition of "business." or "controller". This creates a similar dilemma to the determination of the data controller in the blockchain under GDPR except made even more complicated by (i) the fact that not all entities are may be captureds within the three US state laws subject to CCPA and (ii) the fact that US laws CCPA does not address a situation of co- or joint controllers.

If the blockchain is used for what is deemed under CCPA the US laws as a purchase and sale of personal information or under CPRA to share personal information, a "third party" under CCPA could be implicated if it failed to provide explicit notice and an opportunity to opt out. Finally, a "service provider"/"processor" under CCPA the US laws and a "contractor" under CPRA could be implicated if its actions resulted in a breach by the "business" (similar to the data processor and data controller structure under GDPR).

Under HIPAA, an entity running a blockchain would be in scope if it is a covered entity or a business associate to such entity (see definitions above).

Under GLBA, an entity would be in scope if it is a "financial institution" as defined there or it could be involved as a "service provider"/"processor" similarly to the discussion under CCPA and GDPR.

13. Does the data privacy legislation in your jurisdiction apply to private and permissioned blockchains? If yes, how?

The applicability of data privacy legislation depends first on whether the data involves personal or private information. If it does, depending on the circumstances of the private blockchain, a central operator could qualify as a "business"/"controller" if it has control over the blockchain and determines the purposes and means of processing a consumer's personal information. The same analysis as stated above would apply to determine the applicability of HIPAA or GLBA.

Nodes or miners that help operate the blockchain for the central operator could be considered as service providers under CCPA the US laws or business associates under HIPAA.

14. When public blockchains are used, what main data privacy challenges are raised in your jurisdiction (including but not limited to limit on use, transfer and storage of data)?

The US privacy laws do not contain any specific limitations on this. However, the new laws, for the first time, contain some formulations requiring the processing to be necessary and proportionate and introduce a retention limit, similar to those under GDPR. For example, under CPRA a business' collection and use of personal information must be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes" (1798.100(c)). These obligations have not yet been defined or tested so it remains to be seen whether they will be handled in a similar vein to GDPR.

15. In the absence of official recommendations/interpretations, what are the best practices for processing personal data on both public and private blockchains?

The US Privacy laws are new, and the FTC has not enforced them yet. We are not aware of established practices in the field of data protection in this realm.

16. Have any aspects of the FATF's "travel-rule" been implemented into the AML legislation in your jurisdiction? What kinds of personal data need to be shared by Virtual Asset Service Providers (VASPs) and what kinds of transactions are applicable? (Please try to also answer the question and share your expectations if the legislative works are still in progress.)

The FATF travel-rule is required in the US. The Financial Crimes Enforcement Network (FinCEN), together with the Federal Reserve, issued its own Travel Rule in January 1995, effective May 1996. It was designed to address the AML risks that existed prior to the creation of virtual currency.

On May 9, 2019, the Financial Crimes Enforcement Network (FinCEN) issued guidance, the Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (CVC), which is regularly updated to include additional countries that may pose a risk, to update the original rule to address the unique AML issues presented by virtual currency and to provide certainty concerning the regulatory treatment of virtual assets. This guidance stated that Travel Rule applies to convertible virtual currency and reiterated that the Travel Rule has been in effect for VASPs since 2013. Where FATF uses "virtual assets" and "VASPs," FinCEN's guidance uses money services businesses (MSBs.) and convertible virtual currencies (CVCs).

The guidance says: “The BSA and its implementing regulations require MSBs to develop, implement, and maintain an effective written anti-money laundering program (“AML Program”) that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. The AML program must, at a minimum: (a) incorporate policies, procedures, and internal controls reasonably designed to assure ongoing compliance (including verifying customer identification, filing reports, creating and retaining records, and responding to law enforcement requests); (b) designate an individual responsible to assure day-to-day compliance with the program and BSA requirements; (c) provide training for appropriate personnel, including training in the detection of suspicious transactions; and, (d) provide for independent review to monitor and maintain an adequate program.25 25. 31 USC § 5318(g)(1); 31 CFR. § 1022.320(a)(2).”

In the US, the BSA sets a threshold of $3,000 while the FATF sets a lower one. In October 2020, financial regulators in the U.S. proposed rules to modify the BSA to reduce the general travel rule threshold from $3,000 to $250 for international transfers.

Contact details:

Website inatba.org
Contact contact@inatba.org
Join INATBA membership@inatba.org