Report on Data Privacy Regulations Applicable to Blockchain Technology in Various Jurisdictions Worldwide

By the Privacy Working Group of INATBA

International Association for
Trusted Blockchain Applications

DECEMBER 2020

Contents

1. 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 INATBA Privacy Working Group 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 9 out of the 14 regions (including the European Economic Area as a whole) assessed, there was a reasonable level of legal certainty. Across the remaining five regions, legal certainty was limited when this report was written. Both the United Kingdom and Russia were found to be the most regulated for blockchain purposes. While these 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 which includes the proposed Regulation on Markets in Crypto-assets (MiCA) might have an effect on data protection aspects of asset-related blockchain technology.

2. 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. Such a situation generates a significant burden of verifying compliance of the blockchain-based solution as it is not only one particular data protection regulation to abide by, but potentially multiple. This is especially relevant for large public permissionless blockchains, where there is virtually no control over nodes joining the network from different countries.

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;[1]
- 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";[2]
- 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 (STOA) of the Secretariat of the European Parliament.[3]

Numerous scholars and experts in the field 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 were selected based on their relevance in the blockchain industry and crypto market: The European Union, Brazil, Canada, China, Hong Kong, India, Japan, Russia, Singapore, South Korea, Switzerland, Ukraine, United Kingdom and the United States.

[1] https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

[2] https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

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

We also prepared the following set of questions to be answered based upon the laws of the jurisdictions included in 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 enforce the data protection regulation(s)?
3. Have these authorities issued any specific regulation, guidance or opinions on blockchain? If yes, please summarize.
4. What kind of actors (e.g. data subjects, controllers, processors. . .) do the applicable data protection regulations 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 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 data subjects have under data privacy legislation in your jurisdiction? Does the right to be forgotten exist in your jurisdiction?
12. Which actors in the public permissionless blockchain network 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?

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 which was prepared by the members of INATBA’s Privacy Working Group. It is then followed by country-specific chapters organised in alphabetical order. These chapters were prepared by renowned experts in the field of data protection that agreed to cooperate with the Privacy Working Group on this project.

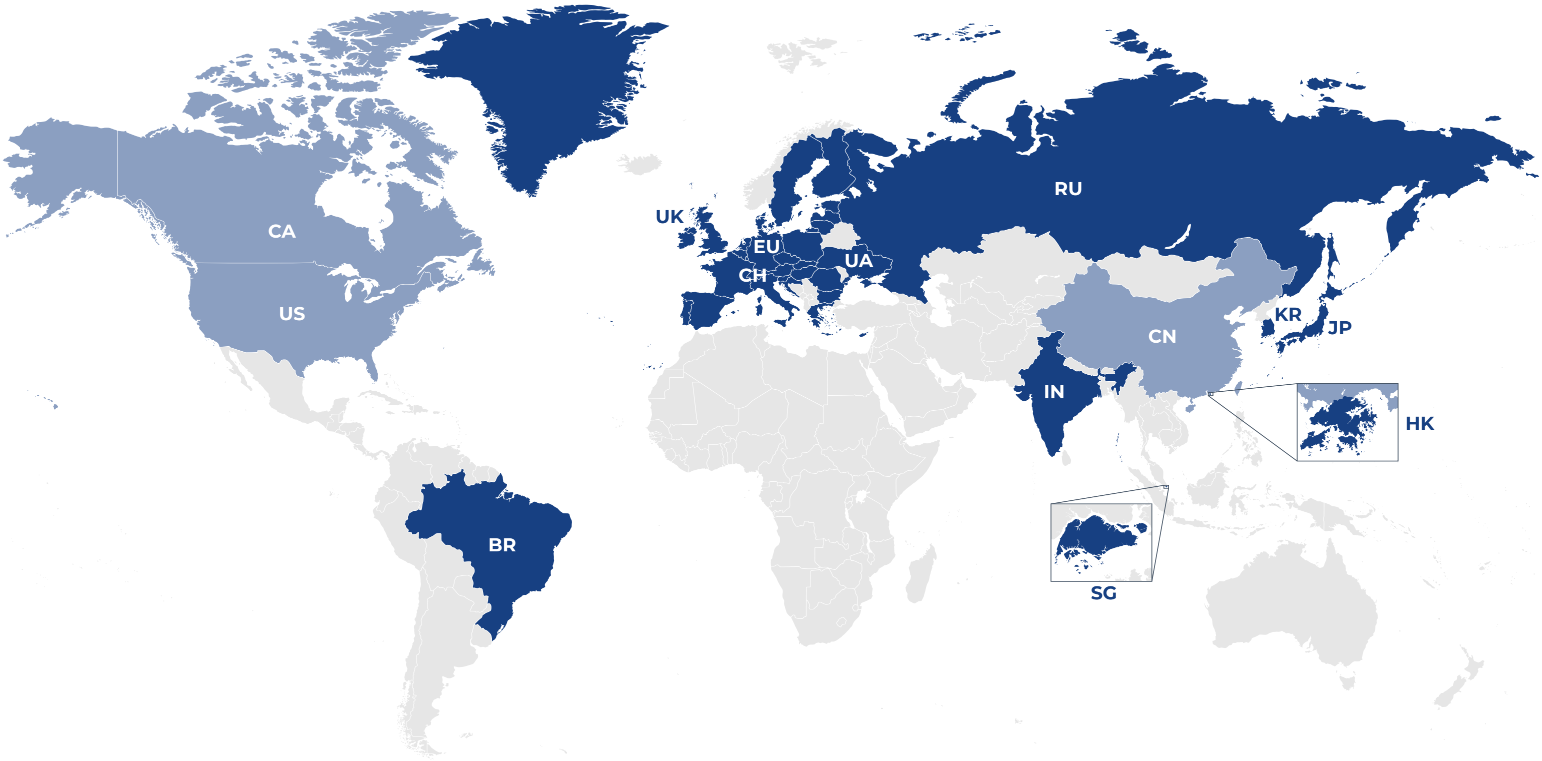
* * *

The International Association for Trusted Blockchain Applications (INATBA) convenes industry actors, startups, SMEs, policymakers, international organisations, regulators, civil society and standard-setting bodies to support mainstream adoption and cross-sectoral upscaling blockchain and Distributed Ledger Technology (DLT) (inatba.org).

The Privacy Working Group of INATBA gathers privacy and blockchain experts from various jurisdictions. The Working Group’s goals are as follows: (i) analyse the applicability of privacy regulations to blockchain technology, (ii) advocate for blockchain-friendly interpretation of privacy regulations and (iii) educate the industry about privacy regulations applicable to blockchain technology.

3. 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 restrictive 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; never-the-less, 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	BR	CA	CN	HK	IN	JP	RU	SG	KR	CH	UK	US	UA
Jurisdictional completeness and precedent														
3. Have authorities specifically addressed blockchain/DLT?	1	0	0	1	0	1	0	0	0	0	0	0	1	0
4. Do data protection rules address specific actors?	2	2	1	2	2	2	2	1	2	2	2	2	1	2
5a. Does data protection define personal data?	2	2	2	2	2	2	2	2	2	2	2	2	2	2
5b. Does it categorize personal data?	2	2	1	0	1	2	2	2	0	2	2	2	2	2

	EU	BR	CA	CN	HK	IN	JP	RU	SG	KR	CH	UK	US	UA
6. Does data protection define pseudo & full anonymisation?	1	2	0	0	0	1	1	2	0	1	0	2	2	2
7a. Is there specific legislation/regulation on blockchain?	0	0	0	1	0	1	1	2	1	1	1	0	1	0
7b. If so, does it refer to data privacy?	0	0	0	0	0	1	1	0	0	0	0	0	0	0
8a. Has anonymization been addressed in the jurisdiction?	0	0	1	0	1	0	1	2	1	1	0	1	1	0
8b. Is such precedent relevant for blockchain?	0	0	1	0	1	0	1	2	1	1	0	1	1	0
Localization and Notification														
9a. Must personal data be stored locally?	0	0	1	1	0	1	0	2	0	0	1	0	0	0
9b. Is international transfer addressed and allowed?	2	2	2	2	2	2	2	2	1	1	2	2	2	2
10. Must authorities be notified of data processing activity?	0	0	0	0	0	0	0	2	0	0	1	2	0	2
Overview of defined rights in data protection rules														
11a. Right to access & corrections?	2	2	2	2	2	2	2	2	2	2	2	2	1	2
11b. Right to be forgotten? Or some deletion?	2	2	0	1	1	2	1	1	0	1	1	2	0	1
11c. Right to restrict processing?	2	2	0	1	1	1	2	2	0	2	2	2	1	1
11d. Obligation of notifications?	2	1	1	1	1	1	1	1	1	2	2	2	1	2
11e. Right to portability?	2	2	1	1	0	2	0	0	0	1	0	2	0	0
11f. Right to object?	2	2	0	2	2	2	2	2	1	2	2	2	1	2
11g. Right to not be subjected to automated decisions?	2	2	2	1	1	1	1	2	0	0	0	2	0	2
Potential applicability of existing rules to blockchains														
12. Would actors in a public permissionless blockchain be responsible?	1	1	0	1	1	2	1	1	0	1	1	2	1	1
13. Does data protection apply to private/ permissioned blockchains?	2	2	2	1	1	2	1	2	2	1	1	2	1	2
Average value	**1.29**	**1.24**	**0.81**	**0.95**	**0.90**	**1.33**	**1.14**	**1.52**	**0.67**	**1.10**	**1.05**	**1.52**	**0.90**	**1.19**

Legend

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

4. Contributors

INATBA Privacy WG

- Marcin Zarakowski, Lisk Foundation (co-chair)
- Silvan Jongerius, TechGDPR (co-chair)
- Anna-Maria Osula, Guardtime
- Jed Grant, KYC3/Infrachain
- Mirjam Kert, Guardtime
- Nathan Vandy, Blockchain HELIX

Brazil

- Tatiana Campello, Demarest Advogados
- Julia Davet Pazos, Demarest Advogados

Canada

- Noah Walters, Dentons
- Chloe Snider, Dentons

China

- Hu Ke, Jingtian & Gongcheng
- Yuan Lizhi, Jingtian & Gongcheng

Hong Kong

- Gabriella Kennedy, Mayer Brown
- Cheng Hau Yeo, Mayer Brown
- Karen H. F. Lee, Mayer Brown

India:

- Ikigai law

Japan:

- Ken Kawai, Anderson Mori & Tomotsune
- Keigo Murai, Anderson Mori & Tomotsune
- Takeshi Nagase, Anderson Mori & Tomotsune
- Huan Lee (Henry) Tan, Anderson Mori & Tomotsune

Russia:

- Maxim Zinovyev, B-152
- Maxim Lagutin, B-152

Singapore

- Dharma Sadasivan, BR Law Corporation

South Korea

- Samuel Yim, Kim & Chang
- Mooni Kim, Kim & Chang

Switzerland

- Carmen De la Cruz Böhringer, De la Cruz Beranek

United Kingdom

- Laura Scaife, Datultacy

United States

- Odia Kagan, Fox Rothschild
- Caroline A. Morgan, Culhane Meadows

Ukraine:

- Vlad Nekrutenko, Legal Nodes

5. EU General Data Protection Regulation

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**)[4] is the most important legal act. 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.

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, 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 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 enforce 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 EDPS or their representatives, is responsible for the 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.

[4] 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).

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. Some of the guidelines issued by Art. 29 WP remain valid today.

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

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.[5] 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.

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.[6]

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.

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. 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] 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.

[6] 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.

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 broad 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,” mentioned 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[7] requires additional protection and may only be collected as an exception, mainly when under the control of an official authority.

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.”

Despite this, it should still be noted that recital 26 specifies that pseudonymous data should still be considered information pertaining to an identifiable natural person. Indeed, with this technique, data subjects can easily be identified when additional information is added to the pseudonymous data. It means that data which was rendered anonymous is still subject to data protection rules. At the same time, pseudonymisation is considered as a technique that helps data controllers and processors to meet their data-protection obligations.[8] 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.[9] The opinion provides further guidance on anonymisation techniques and supports the significantly high

[7] General Data Protection Regulation, *op. cit.*, article 10.

[8] *Ibid.*, recital 28.

[9] 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.

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.[10]

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.

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,[11] the Market Abuse Regulation,[12] the Prospectus Regulation,[13] the Transparency Directive,[14] the Short-selling Regulation[15]). Some payment tokens may also fall under the definition of e-money and would therefore be covered by the EU E-Money Directive[16] and possibly under the PSD 2.[17]

Moreover, the 4th and 5th Anti-Money Laundering Directives[18] impose obligations on EU Member States to have their AML laws at least cover 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,[19] the E-commerce Directive[20] and the Directive on the distance marketing of consumer financial services.[21]

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.

[10] EDPB — Endorsement 1/2018, https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

[11] Directive 2014/65/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0065&qid=1605789164153.

[12] Regulation (EU) No. 596/2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0596&qid=1605789304253.

[13] Regulation (EU) 2017/1129, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1129&qid=1605789369505.

[14] Directive 2013/34/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0034&qid=1605789435888.

[15] Regulation (EU) No. 236/2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R0236&qid=1605789499123.

[16] Directive 2009/110/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0110&qid=1605789567249.

[17] Directive (EU) 2015/2366, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366&qid=1605789614736.

[18] 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.

[19] Directive 2011/83/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0083&qid=1605789799455.

[20] Directive 2000/31/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000L0031&qid=1605789847394.

[21] Directive 2002/65/EC, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32002L0065.

8. Have any particular anonymisation or pseudonymization 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 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."[22]

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."[23] 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 reidentification as well as the reasonable guarantee of system robustness beyond the expected useful life of personal data.[24]

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.

[22] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, p. 3.

[23] GDPR, recital 26. See also: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU%282019%29634445_EN.pdf, p. 31.

[24] https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf, p. 23.

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.

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 article 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. This is relevant because personal data collected has to have a purpose and any change regarding this purpose has to be communicated to and permissioned by the subject.

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 the public permissionless blockchain network would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

Public permissionless 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 mentioning 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.[25]

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.

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

6. Country specific chapters

Brazil

Authors:

- Tatiana Campello, Demarest Advogados
- Julia Davet Pazos, Demarest Advogados

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 September 18, 2020. Note, however, that sanctions related to non-compliance with the LGPD can only be applied from 1 August 2021, as provided for by Law 14,010/20.

2. What authority(ies) are responsible for data protection and enforce 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 regulation, guidance or opinions on blockchain? If yes, please summarize.

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 behavioral 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 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 authorizes 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 operator 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 holder has the right to request that the data is erased/deleted; however, blockchain is a technology known for 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 the public permissionless blockchain network would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

The LGPD only holds the data controller and operator 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 operators.

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: (i) the processing of the operation is carried out within the national territory; (ii) the processing activity has the objective of offering or providing goods or services or processing data from individuals located in the national territory; or (iii) 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 anonymized data, except when the anonymization 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.

Canada

Authors:

- Noah Walters, Dentons
- Chloe Snider, Dentons

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

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, there is also developing common law that imposes civil liability for certain types of privacy breaches.

On 17 November, 2020, the Ministry of Innovation Science and Economic Development introduced Bill C-11 (the Digital Charter Implementation Act). The Bill would replace PIPEDA as the new federal privacy legislation for the private sector by enacting: (1) the Consumer Privacy Protection Act (CPPA), and (2) the Personal Information and Data

Protection Tribunal Act (PIDPT). The Bill draws inspiration from PIPEDA, and the European Union's General Data protection Regulation (GDPR). However, the Bill is still being debated in the House of Commons and it is not yet clear whether it will pass and what it will look like in its final form. Accordingly, the remainder of this section is based on existing legislation, unless stated otherwise.

2. What authority(ies) are responsible for data protection and enforce 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. Under Bill C-11, The CPPA would provide for proceedings before a tribunal that would act as an appeal body from findings and recommendations made by the OPC. This would be a new addition to the federal privacy regime – currently no Tribunal exists.

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

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

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 [26] 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.

Under PIPEDA, "organisations" are broadly defined to include "an association, a partnership, a person and a trade union." An organisation is responsible for personal

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

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:[27]

- 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).

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

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

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."[28]

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 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 recognized that there are increasingly sophisticated means to re-identify information that ostensibly appears to be non-personal. In its Proposals to modernize the Personal Information Protection and Electronic Documents Act,[29] 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 recently with Monero, where one study was able to uncover up to 85% of sender identities (before the 2017 update).[30]

The proposed CPPA would provide some guidance to organizations 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.

[28] www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

[29] https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

[30] 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.].

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.

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 organizations must obtain, and how they must obtain it, see the OPC's Guidelines for obtaining meaningful consent.[31]

- 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.

- 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.[32]

- Right to complain to the relevant data protection authorities

  Individuals must be able to address issues with the designated individual who is accountable for an organization's compliance. Organizations 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.

  Under Bill C-11, individuals are expected to be given some new rights, most notably the right to data portability, and the right of erasure, subject to some prescribed limitations. In the case of data portability, the right will be subject to a data mobility framework.

12. Does the right to be forgotten exist in your jurisdiction?

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. See: Reference re subsection 18.3(1) of the Federal Courts Act under subsection 18.3(1).

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

[32] *Ibid.*

A comparable 'right to be forgotten' is described under Bill C-11 in section 55(1) as "Disposal at an individual's request." This proposed right would require organizations to dispose of personal information when they receive a written request for disposal. The organization may refuse disposal if: (a) disposing of the information would result in the disposal of personal information about another individual and the information is not severable; or (b) there are other requirements of the CPPA, of federal or provincial law, or of the reasonable terms of a contract that prevent it from doing so.

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

14. 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.[33]

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.

[33] 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).

China

Authors:

- Hu Ke, Jingtian & Gongcheng
- Yuan Lizhi, Jingtian & Gongcheng

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

There is no single principal data protection legislation in China. Instead, various laws, departmental rules and national standards exist to protect personal data. 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 **NPC Standing Committee**). 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 data 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**) and the People's Bank of China (the **PBC**). Regulations also have mandatory effects. Although the extent of legal force of regulations is lesser than that of laws, regulations have a higher level of legal force compared to national standards.
3. National standards are formulated and promulgated by the Standardisation 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 mandatory effects, while recommended national standards are not mandatory. The extent of legal force of national standards is lower than that of regulations. Generally, the national standards on personal information protection are considered recommended national standards. Although the national standards on personal information protection do not have compulsory legal effects, they are important references for regulatory agencies.

Provisions on personal information protection are distributed across various legislations. The Law on the Protection of Consumer Rights and Interests (the **CPL**, amended in 2013) stipulates the basic principles for business operators to protect consumers' personal information. The provisions outlined by the CPL regarding personal information protection are fully integrated into provisions of the Cybersecurity Law (the **CSL**, promulgated in 2016).

The CSL is the most important law pertaining to personal information protection and also provides an important foundation for the enforcement activities of regulatory authorities. The CSL applies to network operators that construct, operate, maintain and use networks within the territory of China, and this law stipulates the obligation of network operators to protect personal information. If a network operator violates the obligations of personal information protection, it will result in administrative penalties such as issuing an order to make corrections, warnings, fines, confiscation of illegal gains, suspension of relevant business, suspension of entire business for rectification, closing of websites or revocation of business permits or licenses.

Furthermore, the Criminal Law (amended in 2017) stipulates the crimes of infringing upon Chinese residents' personal information and the corresponding criminal liabilities. This law provides a clear legal basis for heightened constraints on the underground industry suspected of personal information crimes. In the field of civil law, the Civil Code (promulgated in 2020) has a special chapter titled "Right to Privacy and Protection of Personal Information," specifying the definition of privacy rights and personal information, protection principles, legal liabilities, rights of individuals, information processing and other issues. In October 2020, the NPC enacted the draft of the Personal Information Protection Law (the **Draft PIPL**) for public consultation; once the PIPL is passed, it will become China's first primary legislation on the protection of personal information.

In terms of regulations, personal information protection provisions are mainly embodied in the regulations of a specific industry or a special field. In the telecommunications and internet sector, the MIIT enacted "Provisions on Protecting the Personal Information of Telecommunications and Internet Users" in 2013. This regulation provides guidelines on the collection and use of personal information by telecommunications business operators and internet information service providers, as well as the corresponding safety measures. In the financial sector, "Implementation Measures for the Protection of Financial Consumer Rights and Interests," which was promulgated by the PBC in 2016 and later revised in 2020, requires financial institutions to obtain express consent before collecting and using financial information of consumers. It 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.

To protect children and minors, the CAC promulgated the Provisions on Online Protection of Children's Personal Information in 2018 to regulate the personal information of online users under the age of 14.

In addition, China's regulatory authorities have recently paid particular attention to the field of mobile applications. In January 2019, the CAC, MIIT, MPS and SAMR jointly launched a special crackdown campaign against illegal collection and use of personal information by applications. The campaign publicly exposed illegal collection and use of personal information by applications and ordered them to rectify their behaviours. In November 2019, the CAC, MIIT, MPS and SAMR introduced "Methods for Identifying the Illegal Collection and Use of Personal Information by Apps," a document which listed applications known for unlawful or unreasonable collection and misuse of personal information. In July 2020, the MIIT issued the "Announcement on Launching In-depth Special Crackdown Campaign the Infringement of Users' Rights and Interests by Apps," which listed the following behaviours: infringement upon users' rights and interests, including the illegal processing of users' personal information by Apps and SDK, obstacles to creating an account, frequently harassing users, cheating and misleading users and failure to perform duties required by application distribution platforms.

On a national level, 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 for 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 sts an important standard for detailing and supporting the requirements for personal information protection as specified in the CSL.

In practice, if an enterprise violates the PIS Specification, the cyberspace administration authorities may interview the relevant officials of the enterprises and call for a special rectification in the entity's personal information collection behaviours.

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

There is no unified personal information protection regulatory authority in China. Multiple government departments work together to jointly manage personal information protection. To some extent, responsibilities of these 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 is responsible for supervising personal information protection of network operators, and it also coordinates personal information protection as a whole. The CAC carries out their supervisory duties by promulgating policies, interviewing enterprises and holding press conferences.
2. The MPS is responsible for preventing and punishing infringements on residents' personal information. They do so by imposing administrative penalties.
3. The MIIT is responsible for supervising and administering personal information protection in the management of network products and services. They promulgate relevant policies, interview enterprises, hold press conferences and conduct special crackdown campaigns.
4. The SAMR is responsible for supervising and administrating the protection of consumer personal information. This can include issuing policies, holding press conferences and imposing administrative penalties (such as warnings, publicity of illegal collection and uses and fines).

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

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

At present, there are no specific laws 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 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 comply with legal requirements and platform usage specification;
5. Authenticate the users' real identity information based on the organization 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 inspections by 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 country's legal tender. The relevant 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. Websites providing bitcoin 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 organizations 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.

Despite this, the Chinese government is supportive of blockchain technology itself. The government has enacted a series of policies and measures to encourage the development of blockchain technologies in order to guide the application of blockchain technologies in the industry and promote industry 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 endorsed 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 further 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), which was issued by the MIIT, required that blockchain innovation should 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 why strengthening research on blockchain basic technologies and executing the application of blockchain technologies in the financial sector is an imperative field.

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 article 76 of the CSL, "network operators" are the owners and managers of the networks or associated network service providers. 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.

The definition of "network" under the CSL is very broad, incorporating the entire system including hardware, software, data and information. Owners and managers of networks and service providers relying on the systems are considered network operators. According to this definition, hardware manufacturers, system software developers or application software developers are merely responsible for manufacturing hardware, developing software or completing the delivery, and do not "operate" networks. Thus, they are not regarded as network operators.

However, the legislative purpose of the CSL is to ensure cyberspace security. Data protection is only one of its legislative purposes. Different types of network operators bear different responsibilities for data protection, and it is thus necessary to classify network operators. In practice, the owner, manager and service provider of the network may not be the same person or entity, and not all of them may legally process data.

According to the PIS Specification and relevant practice of data law, network operators can be categorised as one of the following three types:

1. Personal Information Controller: In accordance with article 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). It is a core concept and often the starting point for legal analysis, as the personal information controller determines the purpose and method of data processing. A series of obligations and responsibilities under the PIS Specification are carried out around the personal information controller.
2. Entrusted Processor: The concept of "entrusted processor" under article 9.1 of the PIS Specification is derived from the concept of "processor" under GDPR and must be understood *vis-à-vis* the concept of data controller. According to the basic principles of civil law, there is a principal-agency relationship between a controller and a processor. A processor is defined as the institution or individual that processes data under the controller's entrustment.
3. Technical Service Provider: In addition to a personal information controller and entrusted processor, there is another type of network operator that neither determines 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." This includes basic cloud service providers, telecommunications operators, etc.

The Civil Code, which will come into effect on 1 January 2021, does not adopt the concept of "personal information controller" under the PIS Specification. Instead, the Civil Code includes controllers as part of the "information processor" category. The Draft PIPL, when using the terminology laid out in the Civil Code, further uses the concept of "entrusted party" to cover those who process personal information without power to determine the processing activities. The use of different terminology across these documents may cause confusion.

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, article 4 of the 2013 "Provisions on Protecting the Personal Information of Telecommunications and Internet Users" asserts 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." Article 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."*

In later works, the definition of personal information was amended to include two criteria. In addition to "identification," the definition also includes "association." The "association" approach discusses the ability to know a given individual and obtain their further linked 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 article 3.1 of the PIS Specifications enacted in 2016 and revised in 2020, personal information refers to "all kinds of information recorded by electronic means or otherwise, which can, independently or in combination with other information, identify specific natural persons or reflect the activities of specific natural persons." The Draft PIPL also includes "identification" and "association" criteria. Article 4.1 of the Draft PIPL stipulates that personal information refers to all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding anonymised information.

In regard to data classification, some industry regulatory authorities in China have made some attempts in this regard, such as the Data Classification Guidelines for Securities and Futures Industry and the Industrial Data Classification Guidelines. The China Information Security Standardization Technical Committee (the **CISTC**) is also drafting several standards on data classification but has not provided any uniform classification standard on personal information. According to the PIS Specification, personal information is classified as general personal information or personal sensitive information. Personal biometric information is considered a special type of personal sensitive information, specifically:

1. According to article 3.2 of the PIS Specification, personal sensitive information refers to personal information that once leaked, illegally provided or abused, could endanger personal and property safety, easily lead to damaged personal reputation and mental /physical health, or discriminatory treatment, etc. Generally, personal information from children under the age of 14 and information

involving the privacy of natural persons is considered personal sensitive information. In addition, personal information that does not fall into the scope of personal sensitive information is classified as general personal information.

2. In addition, personal sensitive information that also contains a special type of data is considered personal biometric information. The PIS Specification does not explicitly define what comprises personal biometric information; however, it lists individuals' genes, fingerprints, voice prints, palm prints, auricles, irises and facial identification features as components of personal biometric information. Controllers of personal biometric information must follow more strict requirements than those applicable to the collection, use, storage, sharing and transfer of personal sensitive information.

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

There is no definition of anonymisation and pseudonymisation in PRC laws and regulations. Anonymisation and pseudonymisation are only defined in the national standards as follows:

1. Definition of Anonymisation: According to article 3.14 of the PIS Specification, anonymisation is an irreversible technical process that makes personal information of subjects unidentifiable or unassociated. Anonymised personal information is not considered to be personal information.
2. Definition of 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-identifiers) with pseudonyms. Pseudonymisation technology creates a unique identifier for each 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 article 3.15 of the PIS Specification, pseudonymised data is de-identified information, and because it can be combined with other information to re-identify or associate individuals, the pseudonymised data is still considered personal information.

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

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

The ledger layer, the consensus layer, and the smart contract layer of the blockchain system are technical layers that clearly differ from other software solutions. The laws and regulations in China do not mention the ledger layer, the consensus layer, and the smart contract layer, and these technical layers are only mentioned in the Financial Distributed Ledger Technology Security Specification (the **Financial DLT Specification**) promulgated by the PBC in February 2020. This document specifies:

1. The Ledger Layer: the structure of the ledger must be tamper-proof, and the 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 should meet security audit requirements.

2. The Consensus Layer: the consensus module should 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 should be able to reach a unanimous and correct consensus within the required time and produce the correct results. The system shall operate correctly given the constraint that the total number of failure nodes and fraud nodes do not exceed the theoretical limit. Furthermore, the consensus module must 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 should be adopted to control user access to the smart contract, limit erroneous infection and visit the external environment. Smart contracts shall limit complexity, have atomic nature and consistency in their 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. Chinese laws and regulations stipulate as follows in regards to cryptographic algorithms:

1. In October 2019, the NPC Standing Committee enacted the Cryptography Law, which stipulates the definition of cryptography, basic principles of cryptography work, classification management system for cryptography and other important definitions. Commercial encryption is most commonly used in the application of blockchain technology, and commercial encryption is required to uphold and abide by laws, regulations, mandatory national standards and industry technical standards. Commercial encryption is also encouraged to obtain the commercial encryption certification. 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. These products can be sold or provided only after they pass the testing and certification conducted by qualified institutions.
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. They then encouraged commercial encryption product creators 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 a national security review. National security should comply with the requirements of the CSL.

The aforementioned laws, regulations and national standards are not directly related to privacy protection, but 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. Principle of Privacy Protection: Privacy protection measures on the financial distributed ledger shall comply with the basic principles of personal information protection stipulated in the PIS Specification.
2. Privacy Protection Strategy: Transaction information and transaction parties' information shall be disclosed. Identity information of transactional parties must also be identified and authenticated. The identity information of transactional parties shall not be fraudulently used, and at least one of the trading content information and trading parties' information should be encrypted. The participants and auditors should have the ability to decrypt and verify the encrypted information. The transaction verification node is responsible for decrypting and verifying the validity and correctness of encrypted information.
3. Technical Requirements for Privacy Protection: Appropriate technical means for regulating authentication, authorisation, access control, confidentiality, integrity, auditing, monitoring, strategies, etc. should be adopted to ensure that all stages of the private information lifecycle are not obtained by unauthorised third parties. This is also key to protecting the identity of the transactional parties from being identified and fraudulently used.
4. Privacy Protection Monitoring and Auditing: A complete privacy protection audit plan must be formulated. The audit contents should include privacy protection strategies and technical means for privacy protection. The audit plans should include but are not limited to daily monitoring, regular audit and *ad hoc* audit.

8. Have any 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 are no laws, regulations, regulatory documents or national standards defining anonymisation technology. The Institute of Information and Communications Technology, a subsidiary of the MIIT, introduced in article 4.3 of the 201 Big Data Security White Paper 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 anonymisation algorithm aims to solve the following problems: the balance between privacy and usability, efficiency of execution, measurement and evaluation criteria, anonymisation of dynamically republished data and anonymisation of multidimensional constraints. An anonymisation algorithm is widely applied in the field of big data security because it can prevent leakage of sensitive data and ensure the authenticity of published data. The 2018 Big Data Security White Paper is not a legally binding document.

"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 identifiers (or other quasi-identifiers).

Pseudonym creation techniques mainly include identifier-independent pseudonym creation techniques and crypto technology-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 rather independently generated, typically by replacing the original value of the attribute with a random value; (2) crypto technology-based identifier-derived pseudonym creation techniques generate pseudonyms by using cryptography techniques such as encryption or hashing of attribute values, also known as “key encoding” of attributes in the dataset.

These specific techniques used for anonymisation and pseudonymisation have not yet been mentioned in court decisions. 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?

In China, there are no general requirements of localisation of personal information, nor are there general limitations on international transfer of personal information. However, in certain circumstances, localisation is required, and international transfers are limited. For example, article 37 of the CSL stipulates that critical information infrastructure operators (the **CIIO**) shall store personal information and important data collected and produced during operations within the territory of China. When it is necessary to provide personal information to overseas operators due to business needs, a security assessment must be conducted in accordance with the measures formulated by the CAC in concert with relevant departments of the State Council.

In terms of the definition of critical information infrastructure (the **CII**), according to article 3.1 of the “Guidelines for the Security Inspection and Evaluation of Critical Information Infrastructure (Draft)” promulgated by the CISTC in July 2017, the CII refers to information facilities in important industries, such as public communications and information services, energy, transportation, water resources, finance, public services, e-government and other information facilities that may seriously endanger national security, national economy and people’s livelihood and public interests, if they suffer destruction, malfunction or data leakage. According to article 18 of the draft of “Regulations on Protection of Critical Information Infrastructure Security” released by the CAC in July 2017, these include (1) government agencies and organisations in industries such as energy, finance, transportation, water conservation, health and medical treatment, education, social security, environmental protection, public utilities; (2) information networks such as telecommunications networks, radio and television network, internet etc., and organisations which provide cloud computing, big data and other large public information network services; (3) R&D and manufacturing organisations in national defence industries, large facilities, chemical industries, and food and drug industries; (4) press industries such as radio stations, television stations, news agencies; and (5) any other critical industries.

Although article 40 of the Draft PIPL stipulates that CIIO and personal information processors whose processing of personal information meets the criteria specified by the CAC shall store the personal information collected and generated in China within the territory of China, the CAC has not yet specified this criteria.

In addition, there are some industrial rules governing localised storage of data. For example, in the credit investigation industry, article 24 of the “Regulation on the Administration of the Credit Investigation Industry” stipulates that credit investigation agencies must sort, save and process the information they collect within the territory of China. For example, article 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 should be stored and used in Mainland China. In the healthcare industry, article 10 of the Administrative Measures for Population Health Information (Draft) stipulates that health information should not be stored in servers in foreign countries.

Health information from the country's population should also not be hosted or leased on servers in foreign countries.

At present, Chinese laws only require the CIIO to conduct a security assessment before cross-border transfers in accordance with the measures formulated by the CAC jointly with relevant departments of the State Council as stipulated in article 37 of the CSL. However, detailed regulations on security assessment methods for cross-border transfer of personal information have not yet been enacted. Article 23 of the Data Security Law (Draft) (the **DSL**) stipulates that data of controlled items shall be subject to the export control system. Article 33 of the DSL also stipulates that if an overseas law enforcement agency requests data within the territory of China, the overseas agency can only transmit data overseas after submitting a report to the competent authorities and obtaining approval from the competent authorities.

According to the Measures on Security Assessment of Cross-Border Transfer Personal Information (Draft) (the **Measures on Assessment**) released by the CAC in June 2019 after the promulgation of the Measures on Assessment: (1) network operators should apply for security assessment by provincial cyberspace administration before cross-border transfers; (2) the network operators should report cross-border transfers of personal information and contract performance to the provincial cyberspace administration before 31 December each year; (3) in case of any major data security incident, the network operators should also promptly report this to the provincial cyberspace administration at the place where it is located; and (4) the provincial cyberspace administration will organize regular inspections of cross-border transfer of personal information, with a focus on the performance of obligations under contracts and violations of the regulations or damage to the legitimate rights and interests of personal information subjects.

The Draft PIPL also set rules for all processors of cross-border personal information transfer. According to article 38 and article 54 of the Draft PIPL, before the transferring personal information across borders, the processor shall inform personal information subjects, obtain their consent and: (1) pass the security assessment organised by the competent authority, (2) obtain a personal information protection certification by a professional organisation, (3) sign the agreement on cross-border transfer with the overseas personal information recipients to meet the personal information protection standards, or (4) meet other requirements stipulated by laws.

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

The existing laws do not require the notification of processing activities of personal information to any authorities in China.

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

In addition, in accordance with article 40 and article 41 of Draft 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 should apply for approval from the competent authority. CIIO and personal information processors, whose processing of personal information reaches the figures specified by the CAC, must pass the security assessment organised by the authority before providing such information to an overseas party.

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?

Although there is no clear definition of the rights of personal information subjects in laws, regulations and national standards, article 43 and 49 of the CSL, article 9 and 11 of the "Provisions on the Protecting the Personal Information of Telecommunication and Internet Users," article 6 of the "Guidelines for Self-assessment of Collecting and Using Personal Information by Mobile Internet Applications (App)," article 6 of the "Methods for Identifying the Illegal Collection and Use of Personal Information by Apps" and article 8 of the PIS Specification specify the rights of personal information subjects as follows:

1. Right to Access: Personal information controllers shall provide the personal information subjects with the personal information or the types of personal information held, the source of personal information, the purpose for using personal information and the identity or type of third party which has received the above personal information.
2. Right to Rectification: If a personal information subject finds that the personal information held by the controller is incorrect or incomplete, the personal information controller shall provide the personal information subject with the method for requesting rectification of the error or provide supplemental information.
3. Right to Deletion: When the personal information controller collects and uses personal information in violation of laws, regulations, or its agreement with the personal information subject, the personal information subject has the right to request deletion. In cases where the personal information controller illegally shares or transfers personal information to any third party and the personal information subject requests deletion, the personal information controller shall immediately stop the sharing or transfer and notify the third party to delete personal information in a timely manner.
4. Right to Withdrawal of Consent: Personal information subjects should be provided with the means to withdraw their consent to collection and use of their personal information. The personal information subjects have the right to refuse to receive commercial advertisements distributed based on their personal information.
5. Right to Cancel the Account: The personal information controller will provide the personal information subject with a convenient and easy-to-operate method for account cancelation. If manual handling is required after the request for account cancelation is received, the verification and handling shall be completed within the promised time limit.
6. Right to Obtain a Copy: According to the request of the personal information subject, it is suggested that the personal information controller shall provide the personal information subject with a copy of basic held personal information, identity information, personal health and physiological information, and educational and occupational information. If technically feasible, the controller should directly transmit the copies of personal information of the aforementioned types to the third party designated by the personal information subject.
7. Right to Report and Complaint: The personal information controller must establish a complaint management mechanism and a complaint tracking process, and should respond to complaints within a reasonable time.

8. Right to Portability: Although the existing laws and rules have not explicitly stipulated the right to portability, in practice, personal information subjects can realise the right to portability in certain circumstances. For example, personal information subjects can port telephone numbers in the telecommunications industry, and patients can carry their own medical records to different hospitals in the medical sector. However, at present, the right to portability is a controversial right in the theoretical field.

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 to deletion can only be exercised under limited conditions: only when the data controller violates laws, regulations or agreements. 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 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 the public permissionless blockchain network would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

There are no specific provisions on the public blockchain in Chinese laws, regulations and national standards, nor are there any specific personal information protection regulations on the public blockchain. The Financial DLT Specification can apply to the public blockchain in the financial sector, and the CSL can apply to public blockchain in the non-financial sector. 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 as follows:

1. Network operators (which are known as financial distributed ledger operators in the financial industry) will participate in the processing of personal data, According to article 14 of the Financial DLT Specification, financial distributed ledger operators collect, transmit, store, present, inform, de-register and process account information, identification information, transaction information, personal identity information, property information and other information reflecting the activities of specific natural persons.
2. 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 do not directly participate in personal data processing activities. Thus, there is no need for technical service providers to perform the obligations of personal data protection.

According to industry practices, blockchain service providers can be divided into identity authentication service agencies, consensus service agencies, smart contract service agencies, platform service agencies and application service agencies, consensus service agencies, smart contract service agencies and platform service agencies have fewer chances to collect or use personal information. However, neither the CSL nor the Financial DLT Specification classifies types of network operators (or financial distributed ledger operators in the financial industry). Therefore, the laws and national standards require network operators (or financial distributed ledger operators in the financial industry) to assume the obligation of personal information protection.

In addition, data processing agencies in the field of blockchain can be categorised as personal information controllers or entrusted processors. Personal information controllers are capable of determining the purposes and methods of personal information processing and directly enter into service agreements with clients of the blockchain system, directly assuming the obligations of personal information protection. The personal information controller delegates the processing of personal data 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 includes provisions for privacy protection.

Even though there is no specific law or regulation on personal data 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," which aligns with the definition of a network as set forth in the CSL. Since the blockchain can be considered a network along these criteria, the provisions for 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, meaning the regulatory documents on the personal information protection in data processing activities, such as the PIS Specifications, are thus applicable to blockchain service providers.

Hong Kong

Authors:

- Gabriella Kennedy, Mayer Brown
- Cheng Hau Yeo, Mayer Brown
- Karen H. F. Lee, 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: 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 response to recent data breaches and doxxing incidents in Hong Kong and to bring Hong Kong's data protection legislation in line with international developments, the Hong Kong government has also proposed certain amendments to the PDPO. There are six key proposals currently being put forward: (1) the introduction of a mandatory data breach notification regime; (2) the requirement for data users to implement data retention policies; (3) the enhancement of powers of the Office of the Privacy Commissioner for Personal Data (**PCPD**) to tackle doxxing incidents; (4) the direct regulation of data processors; (5) expanding the definition of "personal data"; and (6) a review of the penalties that may be imposed for a breach of the PDPO. These amendments are likely to be introduced in 2021.

2. What authority(ies) are responsible for data protection and enforce 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:

(a) undertake investigations and inquiries and issue enforcement notices in the event of any breach of the PDPO;

(b) enter any premises for investigation or inspection purposes (subject to certain requirements);

(c) 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

(d) 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.

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 regulation, guidance or opinions on blockchain? If yes, please summarize.

No specific regulations or guidelines on blockchain have been published by the PCPD. 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 privacy issues that may arise from the application of blockchain for various purposes. In particular, the article highlights three main privacy risks:

(a) 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 new participants who may later join the network. This may conflict with the basic data protection principle asserting 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.

(b) 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.

(c) 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. In essence, the CNIL suggests that organisations should carefully consider the implications before embarking on adopting blockchain technology and prioritise data minimization 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.

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 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";

(b) "Data user" 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

(c) "Data processor" is defined 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. Furthermore, in cases 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 personal data from being kept longer than necessary for processing, as well as to prevent unauthorised or accidental access, processing, erasure, loss or misuse 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 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 regarding the collection and use of certain types of personal data that is considered to be particularly sensitive and 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 mandate individuals 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, it should be noted that the Hong Kong SFC issued a position paper in November 2019 which set out a new regulatory framework for crypto exchanges and virtual asset trading platforms. For example, licenses 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.

8. Have any 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. In cases 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:

(a) 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);

(b) the transfer is pursuant to the consent provided by the data subject; or

(c) 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 they are 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 their 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 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 the public permissionless blockchain network would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

As a public permissionless 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) as they are 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.

India

Author:

- Ikigai law

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

Presently, there is no specific law dealing with data privacy and protection in India. The Indian data protection and privacy framework is embodied in India's 2000 Information Technology Act (**IT Act**),[34] and the 2011 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, issued under it (**SPDI Rules**).[35]

However, a dedicated personal data protection law is currently under development—this is the 2019 Personal Data Protection Bill (**PDP Bill**)[36] which borrows, to a limited extent, from the EU's General Data Protection Regulation (**GDPR**). The PDP Bill is currently being examined by a Joint Parliamentary Committee[37] comprising members from both houses of 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.[38] The Committee of Experts on Non-Personal Data Governance Framework (**NDP Committee**) released its report on 12 July 2020.[39] The relevant portions of the report are discussed throughout this section.

2. What authority(ies) are responsible for data protection and enforce 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 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 NDP Committee's report recommends the establishment of a Non-Personal Data Authority (**NPDA**). The proposed NDPA will (i) ensure that data is shared for sovereign, social welfare, economic welfare and regulatory and competition purposes; and (ii) ensure all stakeholders follow prescribed rules and regulations, provide data when data requests are made, undertake ex-ante evaluations of the risk of re-identification of anonymised personal data and so on.[40]

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

[35] See https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=GSR313E_10511(1)_0.pdf.

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

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

[38] See https://meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf.

[39] 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-data-governance-framework.pdf.

[40] *Ibid.*, p. 41.

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

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): 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,"[41] which noted:
   - 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.[42]
   - 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.[43]
   - There are cost-saving, transparency, and efficiency advantages of the technology and the time is ripe for its adoption in India.
2. RBI: In January 2019, The IDRBT released a "Blueprint of Blockchain Platform for Banking Sector and beyond,"[44] which noted:
   - 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.
   - A common standardised infrastructure must be set up to facilitate business development of communication networks.
   - 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.
   - 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.
3. RBI: On 11 February 2020, the RBI released a notification, "Distributed Ledger Technology, Blockchain and Central Banks,"[45] which noted:
   - Distributed ledger technology (**DLT**) and blockchain technology have the potential to provide solutions to the financial sector.

[41] See IDBRT whitepaper, available at https://idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf.

[42] *Ibid.*, p. 26.

[43] *Ibid.*, p. 26.

[44] *Ibid.*

[45] See https://m.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=18766.

- Increasing support from RBI and government of India through regulatory sandbox and other mechanisms will help support innovation in blockchain.
- Blockchain technology has characteristic features such as hash function, nodes, blocks and tokens.
- Various developments have taken place with regard to adopting DLT and blockchain by start-ups and financial institutions.[46]

4. Securities and Exchange Board of India (**SEBI**): In August 2017, a Committee on Financial and Regulatory Technologies (**CFRT**) was set up to explore the possibility of implementing blockchain in stock markets.[47]

    - The terms of reference of the CFRT specifically envisage exploring DLT technologies.[48]
    - The CFRT is yet to release its report.

5. NITI Aayog: In January 2020, "Draft Discussion Blockchain: The India Strategy,"[49] was released by NITI Aayog, which noted:

    - Regulatory and policy considerations must be developed for evolving a vibrant blockchain ecosystem.
    - Creation of a national infrastructure for deployment of blockchain solutions with inbuilt fabric, identity platform and incentive platform is recommended.
    - 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.
    - 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.[50]

6. MeitY: IDRBT is engaged in a research project entitled "Distributed Center of Excellence for Blockchain Technology,"[51] sponsored by MeitY. Key objectives of the project include:

    - Evolving a blockchain ecosystem around R&D organisations, government departments and academia.
    - Conducting research on issues and challenges related to blockchain usage in identified application domains and enhancing capacity-building in blockchain technology.
    - The report with the findings of the research project is yet to be released.

7. MeitY: In 2019, MeitY released "India's Trillion-Dollar Digital Opportunity"[52] which noted:

[46] See Table 2 of the notification, available at https://m.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=18766.

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

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

[49] 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.

[50] *Ibid.*, p. 52.

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

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

- 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.[53]
- The private sector in India has started working on blockchain applications such as ICICI Bank, Mahindra, IBM and Bajaj Electricals.

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

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

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.[54]

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 "corporate body" 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):

(13) "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.

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

(15) "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.

NDP Committee Report:

Recommendation 2: Defining non-personal data roles:

Clause 4.7: In the NPD Committee's report, the definition of a "data principal" is related to the type of non-personal data, including public, community and private data, as well as based on different possible kinds of data subjects.

[53] *Ibid.*

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

- In case of public non-personal data: The government may collect data pertaining to citizens (e.g., a census), companies (company registration, financial filings) and communities. The data principal is considered to be the corresponding entities (individuals, companies, communities) to whom the data relates.
- In case of private non-personal data: The private sector may collect data pertaining to citizens (e.g., customer surveys), companies (e.g., vendor registration, vendor product information) and communities. The data principal is considered to be the corresponding entities (individuals, companies, communities) to whom the data relates.
- In case of community non-personal data: A community, that is the source and/or subject of community data and as defined in section 4.3 of the NPD Committee report, may be treated as the data principal for such data, and should be able to exercise key rights, including economic rights, to this data.

Clause 4.8: A "data custodian" undertakes collection, storage, processing, use, etc., of data in a manner that is in the best interest of the data principal.

Clause 4.9: A "data trustee" means the actor who would exercise the data principal group/community's rights on their behalf.

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 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:

(i) password,

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

(iii) physical, physiological and mental health condition,

(iv) sexual orientation,

(v) medical records and history,

(vi) 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,

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

(viii) 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:

(i) financial data,

(ii) health data,

(iii) official identifier,

(iv) sex life,

(v) sexual orientation,

(vi) biometric data,

(vii) genetic data,

(viii) transgender or intersex status,

(ix) caste or tribe,

(x) religious or political belief or affiliation or

(xi) 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 the data other than personal data.

NPD Committee Report

Clause 4.1 (i): Non-personal data means when data is not considered 'personal data' (as defined under the PDP Bill), or the data is without any personally identifiable information (PII), it is considered non-personal data.[55]

Non-Personal Data is further classified into three kinds:

Clause 4.2: "Public non-personal data" means non-personal data collected or generated by the governments, or by any agency of the governments, and includes data collected or generated in the course of execution of all publicly funded works.[56]

Clause 4.3: "Community non-personal data" means non-personal data, including anonymised personal data, and non-personal data about inanimate and animate things or phenomena—whether natural, social or artefactual, whose source or subject pertains to a community of natural persons. Provided that such data shall not include private non-personal data.[57]

Clause 4.4: "Private Non-Personal Data" means Non-Personal Data collected or produced by persons or entities other than the governments, the source or subject of

[55] See Report by the Committee of Experts on Non-Personal Data Governance Framework, *op. cit.*, p. 13.

[56] See Report by the Committee of Experts on Non-Personal Data Governance Framework, *op. cit.*, p. 14.

[57] *Ibid.*, p. 14.

which relates to assets and processes that are privately-owned by such person or entity and includes those aspects of derived and observed data that result from private effort.[58]

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.

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. Furthermore, 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. Lastly, if the relevant application acts as an intermediary as defined in the IT Act, it would also have to comply with the 2011 Information Technology (Intermediaries guidelines) Rules (**Intermediary Rules**).[59] However, the Intermediary Rules do not directly refer to data privacy.

- 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

[58] *Ibid*., p. 15.

[59] See https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=Information%20Technology%20(Intermediaries%20Guidelines)%20Rules,%202011.pdf.

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.

Finally, an Indian High Level Inter-Ministerial Committee that was instituted in 2017 submitted a draft of the Banning of Crypto-currency and Regulation of Official Digital Currency Bill (**Draft Bill**) along with a related report to the government in 2019. The Draft Bill defined cryptocurrencies[60] and DLT,[61] prohibited mining, generating, holding, selling, dealing in, issuing, transferring and disposing of or using cryptocurrency in the territory of India.[62] It further banned the use of cryptocurrency as legal tender and currency[63] and prohibited the use of cryptocurrencies for certain activities.[64] It also listed the activities which would be considered offences[65] under the Draft Bill. While the Draft Bill has not yet been tabled in the Indian Parliament, the Ministry of Finance has moved an inter-ministerial note for consultations on how to regulate cryptocurrencies.[66] This indicates that the government may still be contemplating banning cryptocurrencies in India, however blockchain technology as a whole is likely to remain unaffected.

8. Have any 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.

[60] Clause 2 (1) (a) of the Draft Bill states that "Cryptocurrency, by whatever name called, means any information or code or number or token not being part of any Official Digital Currency, generated through cryptographic means or otherwise, providing a digital representation of value which is exchanged with or without consideration, with the promise or representation of having inherent value in any business activity which may involve risk of loss or an expectation of profits or income, or functions as a store of value or a unit of account and includes its use in any financial transaction or investment, but not limited to, investment schemes."

[61] Clause 2 (1) (e) of the Draft Bill states that "Distributed Ledger Technology means any technology that enables transactions and data to be recorded, shared, and synchronized across multiple data stores or ledgers, or a distributed network of different network participants, through the use of independent computers (referred to as nodes) who record, share and synchronize such transactions and data in their respective electronic ledgers (instead of keeping data centralized as in the case of a traditional ledger)."

[62] Clause 3 (1), Draft Bill.

[63] Clause 6, Draft Bill.

[64] Under clause 7 of the Draft Bill, these prohibited activities included, amongst others, buying, selling or storing cryptocurrency; providing cryptocurrency related services to consumers or investors; and trading cryptocurrency with Indian currency or any foreign currency.

[65] See Clauses 8 and 9 of the Draft Bill.

[66] See https://m.economictimes.com/news/economy/policy/with-a-law-india-plans-lasting-ban-on-cryptos/articleshow/76330403.cms.

The MeitY recently notified a protocol[67] to deal with the data obtained from the Aarogya Setu app, which is India's COVID-19 contact tracing app. As per the protocol, the response data must undergo hard anonymisation, which must uphold anonymisation protocols that will be developed, reviewed and updated on a periodic basis by an expert committee appointed by the Principal Scientific Advisor to the Government of India (point 8 on page 4 of the protocol). That said, unlike the UK ICO,[68] the Personal Data Protection Commission of Singapore,[69] and the Working Party under article 29 of the EU Directive,[70] 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?

Presently, data localisation requirements are applicable only to financial data. The RBI in a circular dated 6 April 2018 entitled "Storage of Payment System Data,"[71] 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."

However, 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 (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 43 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.

The NPD Committee Report recommends that storage of non-personal data should be along the lines of data localisation envisaged in clause 33 of the PDP Bill:[72]

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

(ii) 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.

[67] See https://meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf.

[68] See https://ico.org.uk/media/1061/anonymisation-code.pdf.

[69] See https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf.

[70] See https://www.dataprotection.ro/servlet/ViewDocument?id=1085.

[71] See https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244.

[72] See Report by the Committee of Experts on Non-Personal Data Governance Framework, *op. cit.*, p. 38.

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 processors' or 'data fiduciaries' to report their processing activities to any authority, however, it lists certain additional compliances for 'significant data fiduciaries' (**SDF**).

The DPAI may inform any data fiduciary or class of data fiduciaries of their SDF status 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 compliance criteria applicable to SDFs are (i) registration with the DPAI; and (ii) undertaking a data protection impact assessment (**DPIA**); (iii) maintaining records as specified by regulations issued under the act; (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.

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).

Furthermore, 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).

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).

12. Which actors in the public permissionless blockchain network 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 qualify as a data processor. However, it is more 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.

Japan

Authors:

- Ken Kawai, Anderson Mori & Tomotsune
- Keigo Murai, Anderson Mori & Tomotsune
- Takeshi Nagase, Anderson Mori & Tomotsune
- Huan Lee (Henry) Tan, Anderson Mori & Tomotsune

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

The Act on the Protection of Personal Information[73] (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 5 June, 2020, a bill for the revision of the APPI submitted by the Personal Information Protection Commission (the **Commission**) passed the Diet. 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 increased distribution of data across borders. The 2020 Revised Act provides a definition for "Pseudonymously processed information," defined as 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 Revised Act is expected to take effect by Spring 2022.

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

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

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

No specific regulation, guidance or opinion on data protection in the area of blockchain has 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 APPI defines a "Personal Information Handling Business Operators" as a business operator (whether an individual or corporation) that utilises

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

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.

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 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, including 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 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 is defined as 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 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 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 for pseudonymisation. However, the 2020 Revised Act, which has been approved by the Cabinet, defines "Pseudonymously processed information" in article 2, paragraph 9 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 following categories of personal information:

(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 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 to notify data subjects of the purposes for which their personal data will be used in writing.

8. Have any 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,"[74] Additionally, the Commission is expected to issue guidelines on pseudonymisation techniques before the 2020 Revised Act comes into effect.

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

In general, there is no legal requirement for personal data to be stored in Japan. That being said, article 19 of the 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

[74] https://www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf.

personal data without delay when their utilisation has become unnecessary. In addition, article 20 of the APPI requires Personal Information Handling Business Operators to take action when 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 light of the security concerns involved in such methods 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 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.

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 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 enquire 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 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 was acquired in violation of the provisions of article 17 of the 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 30, paragraph 5 of the 2020 Revised Act, to request for Personal Information Handling Business Operators to suspend their use of personal data or suspend the provision of 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 22–2, paragraph 1 (i.e., leakage or other disclosure) 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 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, the 2020 Revised Act contains no provisions in respect of the right to be forgotten.

12. Which actors in the public permissionless blockchain network 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 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 which 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 APPI which restricts the international transfer of personal data without a data subject’s prior consent and/or article 16 of the 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.

Russia

Authors:

- Maxim Zinovyev, B-152
- Maxim Lagutin, B-152

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 enforce 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 regulation, guidance or opinions on blockchain? If yes, please summarize.

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 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"[75] 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 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 defense 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;

[75] https://digital.gov.ru/en/personaldata/.

(f) list of actions (operations) performed with personal data and a general description 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 purposes 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 the public permissionless blockchain network 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,"[76] 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.

[76] Any information relating to directly or indirectly identified or identifiable natural person ("subject of personal data").

Singapore

Author:

- 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 out the law on personal data protection in Singapore.

2. What authority(ies) are responsible for data protection and enforce 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 regulation, guidance or opinions on blockchain? If yes, please summarize.

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**),[77] 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." A Bill was recently passed on 04 January 2021 to further enhance the PSA to include regulation of virtual payment providers who facilitate the transmission, exchange or storage of digital payment tokens.

8. Have any 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.

[77] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf.

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 organizations 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 a 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 the public permissionless blockchain network 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.

South Korea

Status as of 1 June 2020

Authors:

- Samuel Yim, Kim & Chang
- Mooni Kim, Kim & Chang

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

In South Korea, protection of personal information is primarily governed by the Personal Information Protection Act (the **PIPA**) and various sector-specific laws. For example, the Act on Promotion of Information and Communications Network Utilization and Information Protection (the **Network Act**) applies to the collection, use and processing of personal information of online users while the Credit Information Use and Protection Act (the **Credit Information Act**) would apply to collection, use and processing of personal credit information by, for example, financial institutions and electronic financial companies.

Amendments for the PIPA (together with the original PIPA, the **Amended PIPA**) and Credit Information Act were passed in January 2020. The Amended PIPA is scheduled to take effect in August 2020. The amended Credit Information Act will generally become effective in August 2020 (with some provisions to become effective in 2021).

Our responses below focus on the PIPA and the Network Act (not the Credit Information Act) unless otherwise specified.

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

The Ministry of the Interior and Safety and the Korea Communications Commission are currently responsible for enforcement of the PIPA and the Network Act, respectively.

However, with the effect of the Amended PIPA, the Personal Information Protection Commission (the **PIPC**) will be the central administrative agency for enforcement of the data protection laws.

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

No. There has been no such regulation, guidance or opinions on blockchain made by the data protection authorities.

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.

“Data controller”: PIPA uses the term “personal information controller” to refer to a public institution, corporate body, organisation or individual who manages personal information directly or by liaison.

“Data processor”: The PIPA also includes the concept of a “delegatee,” defined as a person who is delegated with the responsibility to process personal information,and is only responsible for compliance with more limited aspects of the PIPA.

“Data subject”: The PIPA uses the term “data subject” to mean an individual who is identifiable by the information processed hereby becoming the subject of that information.

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

Under the PIPA, “personal information” is broadly defined as information pertaining to a living individual which identifies a specific person by name, address, image or similar identifier.

“Sensitive personal information” is defined as the beliefs, joining or withdrawal from a labour union or political party, political opinions, health, sexual life and other personal information prescribed by the Presidential Decree which could substantially infringe on the privacy of a data subject. The Amended PIPA and the related Presidential Decree would expand the scope of sensitive personal information to include any information on an individual’s physical, physiological, behavioral characteristics collated/ created by certain technological means and any information on race or nationality whose processing (on a case-by-case basis) raises a concern for unjust indiscrimination against an individual.

“Unique identification information” is information bestowed on an individual for identification, such as a resident registration number, passport number or driver’s license number.

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

The Amended PIPA introduces the concept of “pseudonymised information,” a subset of personal information. The Amended PIPA defines pseudonymised information as personal information which has been partially deleted or partially/wholly substituted so that the information can no longer identify an individual without utilisation of or combination with additional information to restore the information to its original state. The Amended PIPA allows a personal information controller to process pseudonymised information for such purposes as statistical analysis, scientific research (research that applies scientific methods, including development and evaluation of technology, basic research, applied research and private sector research) and preservation of public records, without the data subject’s consent, provided that where such pseudonymised information is provided to a third party without the data subject’s consent, such pseudonymised information cannot be provided together with information that can be used to identify a specific living individual.

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

The Partial Amendment to the Act on Reporting and Using Specified Financial Transaction Information (the **Amended AML Act**) was passed by the National Assembly in March 2020. The Amended AML Act, the first law in Korea to specifically address cryptocurrency-related activities, will impose anti-money laundering requirements for cryptocurrency exchanges and other virtual asset service providers (each referred to as a **VASP**) from March 2021. The Amended AML Act does not refer to data privacy other than the requirement for a VASP to obtain an information security management system certification of its IT systems pursuant to the Network Act.

8. Have any 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 Amended PIPA has introduced the concept of anonymised/pseudonymised data, but there is no guideline with further details yet.

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

General provisions apply to personal information controller:

- In Korea, there is a distinction between (i) provision of personal information to a third party (where the recipient intends to use the information for their own purposes) and (ii) delegation of personal information for processing where a third party (e.g., cloud service providers) is delegated to process personal information on behalf of the data controller to perform specific obligations pursuant to the underlying delegation contract.
- If the personal information is to be provided to a third party overseas, the personal information controller must notify the data subject of the following when obtaining consent:

  (i) Identity of the third party (with contact information) to which the personal information is to be provided and country if the third party is an overseas entity;

  (ii) Purpose behind the use of the personal information by the third party;

  (iii) Specific items of personal information to be provided;

  (iv) Time period of retention and use by the third party; and

  (v) Right to refuse and any disadvantages stemming from refusal.
- As discussed above, third parties are deemed to be any entity which may be receiving and/or sharing the information and processing it for its own purposes (in contrast to delegation of processing arrangements where the information is used solely for the benefit of the entity entrusting such information). Special consideration is not given to affiliated entities.
- Although consent is required in principle for offshore data transfers, such a requirement does not apply to delegation of personal information processing that entails offshore retention. Instead, there are other requirements that apply to delegation including entering into a delegation agreement with specific provisions set out in the data privacy laws and disclosing certain details of such delegation (e.g., the name of the delegated company and purpose of delegation) on its website.

Special provisions applicable to online service providers (OSPs):

- If personal information will be transferred to an overseas entity (regardless of whether the transferee is an affiliate or an unrelated party), the OSP must obtain consent from the data subjects after disclosing the *following* items:

  (i) the specific information to be transferred overseas;

  (ii) the destination country;

(iii) date, time and method of transmission;

(iv) the name of the transferee and the contact information of the person in charge of the personal information within the transferee; and

(v) the purpose of the use of the personal information by the transferee and the period of retention and usage.

In this case, the term "transfer" covers provision (including access), delegation and storage.

- For overseas delegation and/or storage (but not for provision), this consent requirement may be exempted from requirements if such overseas transfer is necessary to carry out its contractual obligation to users for the benefit of them. In the Amended PIPA, the condition stipulating the necessity to carry out contractual obligations has been deleted and any overseas delegation and/or storage by the OSPs upon the effect of the Amended PIPA would not trigger the consent requirement.
- The requirements for the OSPs to disclose certain information of such transfer (presented above) in their privacy policies would apply regardless of whether the consent requirement is triggered.

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

Notification of processing activities to the authorities is not required but the personal information controller must obtain explicit and prior consent from the data subjects pursuant to the requirements of the PIPA for any and all collection, use and processing activities (subject to certain exceptions).

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, among others, under the data privacy laws of Korea:

- The personal information controller must issue a privacy policy or provide certain information as required under the data privacy laws of Korea for the data subject to make an informed decision on providing consent.
- The data subject may request that they review or copy the personal information held by the personal information controller.
- There is no right to data portability in the PIPA. However, according to the amended Credit Information Act, the data subject will have the right of data portability with respect to their personal credit information (i.e., to demand credit information providers/users to transfer their personal credit information to certain third parties, such as credit rating agencies or credit information providers/users specified in the Presidential Decree).
- The data subject has the right to object or revoke their consent.
- The data subject may request that their personal information be no longer processed and in such case, the personal information controller must cease to process this personal information.
- The data subject who has reviewed the personal information held by the personal information controller may request that their personal information be corrected or deleted. However, there are certain instances which limit this right to be forgotten, such as when retention of personal information is required by law.

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

Anyone that would be deemed as personal information controllers would be subject to the data privacy laws of Korea. However, Korean laws or regulations have yet to address this specific issue.

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

The data privacy laws of Korea would apply the same to private and permissioned blockchains as it would apply to the public permissionless blockchains. However, it is currently unclear as to how Korean privacy laws will apply to private and permission blockchains.

Switzerland

Status as of 1 July 2020

Author:

- Carmen De la Cruz Böhringer, De la Cruz Beranek

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**) [78]
- Ordinance to the Federal Act on Data Protection (SR 235.11) [79]

Additionally there are provisions in several individual regulations.

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

- Federal Data Protection and Information Commissioner (**FDPIC**) [80]
- The cantons additionally have a data protection officer [81]
- Federal and cantonal Data Protection Offices as well as the corresponding courts

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

No.

But the government wants to further improve the framework conditions for companies in the area of blockchain and distributed ledger technology (DLT).[82] 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 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.[83] 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.

[78] 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.

[79] https://www.admin.ch/opc/en/classified-compilation/19930159/index.html.

[80] https://www.edoeb.admin.ch/edoeb/en/home.html.

[81] https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/schweiz.html.

[82] https://www.efd.admin.ch/efd/en/home/themen/Digitalisierung/blockchain.html.

[83] https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-77252.html.

- 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 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 anonymization and/or pseudonymization?

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 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:

  a. They regularly process sensitive personal data or personality profiles; or

  b. 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 the public permissionless blockchain network 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.

Ukraine

Author:

- Vlad Nekrutenko, Legal Nodes

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

- Council of Europe's Convention 108 for the protection of individuals with regard to the processing of personal data;
- Constitution of Ukraine (article 32);[84]
- Law of Ukraine "On Protection of Personal Data" No. 2297-VI of 2010;[85]
- Law of Ukraine "On Information" No. 2657-XII of 1992;[86]
- Law of Ukraine "On Information Protection in Information Telecommunication Systems" No. 80/94-BP of 1994;[87]
- Law of Ukraine "On the Access to Public Information" No. 2939-VI of 2011.[88]

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

According to article 22 of the Law of Ukraine "On Protection of Personal Data," the competent authority is the Ukrainian Parliament Commissioner for Human Rights (**Ombudsperson**).[89]

The Ombudsperson's role is being criticised due to the lack of effective enforcement instruments, as well as its dependence on the Ukrainian Parliament. Until 2014, there was a State Service for personal data protection, which was liquidated due to a lack of independence.

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

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.

Article 2 of the Law of Ukraine "On Protection of Personal Data" defines the following roles:

[84] https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

[85] https://zakon.rada.gov.ua/laws/show/2297-17.

[86] https://zakon.rada.gov.ua/laws/show/2657-12.

[87] https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

[88] https://zakon.rada.gov.ua/laws/show/2939-17.

[89] http://zakon4.rada.gov.ua/laws/show/776/97-%D0%B2%D1%80.

- "Personal data subject" is an individual whose personal data is processed;
- "Personal data controller" means 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" refers to 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" means a natural or legal person to whom personal data is provided, including a third party;
- "Third Party" is 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?

Article 2 of the Law of Ukraine "On Protection of Personal Data" defines personal data as information or a set of information about an individual who is identified or can be specifically identified.

Article 11 of the Law of Ukraine "On Information" defines this concept as confidential Information about the individual 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 considered confidential information.

Article 7 of the Law of Ukraine "On Protection of Personal Data" mentions 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 article 9 of the Law of Ukraine "On Protection of Personal Data," categories of personal data that when processed requires notification of the regulatory body (Ombudsperson), along with special categories defined in Articel 7, also include information about administrative offences, 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?

Article 2 of the Law of Ukraine "On Protection of Personal Data" defines depersonalisation of personal data as 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 has been issued to date.

The current version of AML Law addresses virtual assets providers as subjects of financial monitoring. However, nothing similar in the field of personal data protection has been issued.

However, a number of draft legislative initiatives have been developed. One of the examples is Draft Law No. 7485 dated 15 January, 2018 "On Digital Economy Development."[90]

None of these initiatives have been adopted by the Ukrainian Parliament to date.

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

No.

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 personal data in Ukraine.

However, there is a specific requirement for processing State information, resources or information with limited access, the protection of which is established by law. In accordance with article 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 article 29 of the Law of Ukraine "On Protection of Personal Data," international transfers are allowed based on the following criteria:

- The country of the recipient provides adequate personal data protection. The following countries are considered adequate under article 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 consent for 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 public interest, establishment, performance and ensuring a legal claim;

[90] http://www.fst-ua.info/wp-content/uploads/2019/01/Cryptocurrency_Paper_Sept2018_en.pdf.

(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 article 9 of the Law of Ukraine “On Protection of Personal Data,” it is required to notify the Commissioner (Ombudsperson) on 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?

Article 8 of the Law of Ukraine “On Protection of Personal Data” provides data subjects with the right to:

1) know about the sources of collection, location of their personal data, purpose of processing, location or place of residence of the personal data controller or processor or be given 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 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 could disgrace the honor, 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 the public permissionless blockchain network would be regulated/responsible under the data privacy legislation in your jurisdiction and how?

No specific regulation regarding blockchain actors has been issued in Ukraine to date. As a part of general discussion regarding the application of personal data in a distributed environment, one can infer the following distribution of processing roles:

- Blockchain users (participants) will be regulated as personal data controllers or processors depending on the particular use case;
- Developers and providers of applications 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 considered as 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 controllers are obligated to:

- possess one of the legal grounds provided in article 11 of the Law of Ukraine “On Protection of Personal Data”;
- notify the Commissioner (Ombudsperson) of 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.
- comply with the data protection principles provided in article 6 of the Law of Ukraine “On Protection of Personal Data”;
- comply with the data subject rights provided in article 8 of the Law of Ukraine “On Protection of Personal Data”;
- protect personal data from accidental loss or destruction, from illegal processing, including illegal destruction or access to personal data;
- notify the personal data subject about the data processing, including about the transfer of personal data to third parties;

- delete or destroy the personal data upon one of the conditions specified in article 15 of the Law of Ukraine "On Protection of Personal Data";
- 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) for the processing of personal data that requires the notification to the Commissioner (Ombudperson);
- comply with international transfer requirements provided in article 29 of the Law of Ukraine "On Protection of Personal Data."

Personal data processors are obligated to:

- only process personal data when allowed, meaning for the purpose and in the scope specified in the agreement with the personal data controller;
- comply with the data protection principles provided in article 6 of the Law of Ukraine "On Protection of Personal Data";
- delete or destroy personal data received from the personal data controller upon the end of relationships with the controller;
- protect personal data from accidental loss or destruction and from illegal processing, including illegal destruction or access to personal data;
- destroy personal data upon the request of the data subject if those personal data are processed unlawfully or are inaccurate;
- rectify personal data upon the reasoned request from the data subject;
- 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) for the processing of personal data that requires the notification to the Commissioner (Ombudperson).

Only a state- or commune-owned enterprise is entitled to process personal data on behalf of the state or local authority bodies;

Article 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?

Generic 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 response to the previous question.

United Kingdom

Status as of 1 June 2020

Author:

- Laura Scaife, Datultacy

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

- General Data Protection Regulation (EU) 2016/679 (**GDPR**);
- Data Protection Act 2018 (**DPA 2018**);
- Data Protection, Privacy and Electronic Communications (**Amendments etc.**);
- (EU Exit) Regulations 2019 (SI 2019/419) (**DP Brexit Regulations**).

2. What authority(ies) are responsible for data protection and enforce 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 regulation, guidance or opinions on blockchain? If yes, please summarize.

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.[91] 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.[92] 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 focused on privacy and data protection, including key privacy challenges of new technologies such as blockchain);[93, 94]
- a beta regulatory sandbox scheme which provides support to organisations developing innovative technologies;[95]

[91] https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2013820/esa-big-data-consultation-ico-response-20170321.pdf.

[92] https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf.

[93] https://ico.org.uk/about-the-ico/what-we-do/grants-programme-2018/.

[94] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-launches-latest-phase-of-privacy-innovation-grants-programme/.

[95] https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/.

- a Technology Strategy from 2018–2021 to produce reports and address emerging risks and opportunities arising from technology.[96]
- **British Blockchain Association.** The British Blockchain Association (BBA), a not-for-profit, promotes the adoption of blockchain technology across the public and private sectors by publishing research among other operations.

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 and DPA 2018 have largely similar definitions.

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.
- "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 enactment 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 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 GDPR and the DPA 2018 identify three sets of personal data.

[96] https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf.

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 opinions, 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 GDPR.
- "Criminal conviction data" has the same meaning as in the GDPR.

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

GDPR definitions:

- "Anonymisation" refers to the processing of personal data in such a manner that the data subject is not or no longer identifiable.
- "Pseudonymisation" means 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.

There are no specific definitions in the DPA 2018, the GDPR definitions apply. This must however be considered in the context of Brexit. Paragraph 1 of Schedule 5 to the European Union (Withdrawal Agreement) Act 2020 defers the effect of EU exit Statutory Instruments so that UK law does not diverge from EU law during the transition period.

Therefore although the UK left the EU on 31 January 2020, the GDPR continues to apply in the UK until the end of the UK–EU transition period (**transition period**), alongside the DPA 2018). The legislation must therefore be read together.

When the transition period ends, the changes made by the "Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019" (SI 2019/419) (**DP Brexit Regulations**) will take effect (subject to any further changes made during the transition period). The DP Brexit Regulations will put a new UK GDPR on a statutory footing, and the existing GDPR will be referred to as the EU GDPR in the UK.

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.

There is, however, guidance as to the legal status of blockchain as property. 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.[97]

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 "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).

Public authorities:

Public authorities cannot rely on the legitimate interests ground for tasks performed in the public interest, and must instead rely on other grounds such as that the processing is necessary for the performance of a task carried out in the public interest (article 6(1)(e) GDPR).

Under the 2018 DPA, section 7 explains the test for when an organisation is deemed a public authority:

Meaning of "public authority" and "public body"

(1) For the purposes of the GDPR, the following (and only the following) are "public authorities" and "public bodies" under the law of the United Kingdom—

(a) a public authority as defined by the Freedom of Information Act 2000,

(b) a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (asp 13); and

(c) an authority or body specified or described by the Secretary of State in regulations, subject to subsections (2), (3) and (4).

(2) An authority or body that falls within subsection 1 is only considered a "public authority" or "public body" for the purposes of the GDPR when performing a task carried out in the public interest or in the exercise of official authority vested in it.

The DPA 2018 supplements the conditions in article 6 of the GDPR with additional public interest conditions, for example in relation to risk assessment systems for crime and taxation involving the unlawful use of public money or unlawful claims for

[97] https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf.

payment from public money.[98] Public authorities should therefore carefully consider the additional processing grounds when determining which would apply for the purposes of deploying blockchain technologies, notably where personal data may have been gathered for narrow purposes.

8. Have any 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?

Presently, there is no legal certainty as to which techniques or combination of techniques will meet the threshold of anonymisation under the GDPR and DPA 2018.

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.

The ICO has produced an anonymisation code of practice under the DPA 1998,[99] which is now outdated. In the big data context, the ICO has suggested that anonymisation should be seen as a tool that assists big data analytics and helps organisations with research and development while protecting individuals.[100]

The 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.[101] 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.[102] This, combined with other pseudonymisation techniques, 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

[98] DPA 2018, para. 3, Schedule 2.

[99] https://ico.org.uk/media/1061/anonymisation-code.pdf.

[100] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

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

[102] https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html.

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 the public permissionless blockchain network 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).

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., para. 6801 et seq., and the Fair Credit Reporting Act (**FCRA**), 15 U.S.C. para. 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., para. 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[103] 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.[104]

At the state level, there are 50 separate data breach notification laws. In addition, at least 25[105] states have laws addressing information security of private sector entities. A number of states including California,[106] Delaware[107] and Nevada[108] 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, paras 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.[109] 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

[103] The first case tagged with "privacy and security" on the FTC's enforcement website is a 1997 case that cites section 5. https://www.ftc.gov/enforcement/cases-proceedings/962-3086/brunos-inc-matter.

[104] 15 U.S.C., para. 45(a)(1).

[105] https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[106] California Online Privacy Protection Act ("CalOPPA"), Cal. Business & Professions Code, paras 22575–79 (2004).

[107] Delaware Online Privacy and Protection Act ("DOPPA"), 80 Del. Laws, c. 148.

[108] Nevada Revised Statutes, Chapter 603A.

[109] https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

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 and businesses must comply with CCPA in the meantime.

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).

2. What authority(ies) are responsible for data protection and enforce 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 regulation, guidance or opinions on blockchain? If yes, please summarize.

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, whom 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. 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.[110]
- 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

[110] https://www.ftc.gov/news-events/blogs/techftc/2018/03/its-time-ftc-blockchain-working-group.

amendments to current legislation that blockchain may impact.[111] Moreover, the Attorney General of Vermont established a Blockchain Working Group to determine whether blockchain specific legislation is necessary to protect consumers.[112]

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:

- 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."[113]

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.

[111] https://www.govops.ca.gov/blockchain/.

[112] https://ago.vermont.gov/blog/2018/12/10/attorney-general-and-state-agencies-launch-working-group-to-study-blockchain-technology/.

[113] 45 C.F.R., para. 160.13.

- 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., para. 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., para. 1843 [in certain circumstances.]"[114]

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[.]"[115]

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.

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 license 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.[116]

[114] 15 U.S.C., para. 6809, quoting para. 1843(k) of title 12.

[115] California Consumer Privacy Act (CCPA), 1798.140

[116] N.Y. Gen. Bus. Law, para. 899-aa.

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." [117]

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.[118]

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."[119] 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.

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." [120]

[117] https://www.law.cornell.edu/cfr/text/16/313.3.

[118] https://www.law.cornell.edu/cfr/text/45/160.103.

[119] CCPA, *op. cit.*, 1798.140(o)(1).

[120] CCPA, *op. cit.*, 1798.140(h).

- "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."[121]
- "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 organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer."[122]

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.

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

In 2019, 28 states introduced legislation relating to blockchain.[123] Some states have enacted legislation that supports the use of blockchain technology largely in the digital assets or smart contract space.[124] 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.[125] Multiple states have created blockchain working groups[126] 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.[127] 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."

[121] *Ibid.*, 1798.140(a).

[122] *Ibid.*, 1798.140(r).

[123] https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2019-legislation.aspx.

[124] https://blockchainlawguide.com/resources/2019-05-16---State-Legislature-Blockchain-Report-Card.pdf.

[125] https://www.globenewswire.com/news-release/2018/05/08/1498672/0/en/Colorado-Passes-Blockchain-Technology-Legislation-Supported-by-Filament.html.

[126] https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2019-legislation.aspx.

[127] https://www.legis.nd.gov/assembly/66-2019/documents/19-0323-03000.pdf.

Otherwise, to the extent personal information is included in the blockchain venture, CCPA/CPRA would apply. As you can see above, the definition of personal information is broad and includes online and electronic identifiers.

8. Have any 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 (see above). As CCPA is new and CPRA has not yet taken effect, this has not been tested in court.

Under HIPAA, PHI can be deidentified using the Expert Determination Method[128] and the Safe Harbor Method.[129] 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 harmonize 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.[130]

The preeminent US standards entity, NIST, has published a guide[131] on deidentification techniques and a draft guidance[132] for de-identifying government data sets.

The CCPA definition 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 implantation, 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 localized and does 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

[128] Health Insurance Portability and Accountability Act (HIPAA), para. 164.514(b)(1).

[129] HIPAA, *op. cit.*, para. 164.514(b)(2).

[130] https://www.law.cornell.edu/cfr/text/16/313.3.

[131] https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

[132] https://csrc.nist.gov/publications/detail/sp/800-188/draft.

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 licenses to third parties the brokered personal information of a consumer that the business has no direct relationship with.[133] 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.[134]

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 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,[135] (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.

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.[136]

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.[137]

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

To the extent CCPA 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." This creates a similar

[133] 9 V.S.A., para. 2430(4).

[134] California Civil Code (Cal. Civ. Code), para. 1798.99.80.

[135] Cal. Civ. Code, *op. cit.*, para. 1798.105.

[136] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf.

[137] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/financial-privacy-rule.

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 subject to CCPA and (ii) the fact that CCPA does not address a situation of co- or joint controllers.

If the blockchain is used for what is deemed under CCPA 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" under CCPA 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" 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" 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 or business associates under HIPAA.

Contact details:

Website	inatba.org
Privacy WG Co-chairs	privacy-wg-cochair@inatba.org
Join INATBA	membership@inatba.org