Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Asia Pacific developments

Gabriela Kennedy

Mayer Brown JSM, Hong Kong

1. China

1.1. *The "Gold" standard – China finalizes the long-anticipated standard contract under the Personal Information Protection Law*

1.1.1. *Introduction*

The Cyberspace Administration of China ("**CAC**") issued the Measures on Standard Contracts for the Export of Personal Information ("**SC Measures**") on 24 February 2023, finalizing the hotly-anticipated standard contract for the export of personal information ("**Standard Contract**") under the Personal Information Protection Law ("**PIPL**"). The Finalized Measures come after more than a year since PIPL was brought in, and almost eight months after the release of the Draft Provisions on Standard Contracts for the Export of Personal Information ("**Draft Standard Contract Provisions**").

The finalized Standard Contract becomes effective on 1 June 2023, but with a 6-month grace period (until 30 November 2023) for personal information exports which commenced prior to 1 June 2023.[1] Personal information processors[2] ("**data controllers**") eligible to rely on the Standard Contract (see below section on ***Application***) are expected to revise their data export processes and procedures within the grace period to comply with the SC Measures and the Standard Contract.

1.1.2. *Background*

Under Article 38 of the PIPL, there are three mechanisms that data controllers may utilize in order to export personal information outside of the People's Republic of China ("**PRC**"): (i) the Security Assessment; ii) the Certification or iii) the Standard Contract.

The Security Assessment was finalized by the CAC last year and took effect on 1 September 2022, while a revised draft Certification specification was recently released on 8 November 2022 and finalized on 16 December 2022.

The requirements under the Security Assessment are onerous and mandatory for data controllers that process or export personal information over a certain threshold, or, are deemed to be critical information infrastructure operators ("**CIIOs**"), while the Certification appears to be designed mainly for intra-group transfers.

Accordingly, the Standard Contract is likely to be the most widely used mechanism for exporting data out of the PRC. In this legal update, we look at the key provisions of the finalized Standard Contract and the SC Measures.

1.1.3. *Scope of application*

Under the SC Measures, data controllers must fulfil all the following criteria in order to be able to use Standards Contracts for the export of data. They must be:

1. An entity not classified as a CIIO;
2. Data controllers processing the personal information of less than 1 million data subjects;
3. Data controllers who have exported:
   a. the personal information of **less than** 100,000 data subjects; or
   b. the sensitive personal information of **less than** 10,000 data subjects,

since January 1 of the previous year; and

4. Also not fall within other circumstances as may be specified by other laws, regulations and rules.

However, the SC Measures now prohibit data controllers from dividing data exports into separate batches to circumvent the Security Assessment.[3] This was previously unaddressed in the Draft Standard Contract Provisions and seemed

E-mail address: gabriela.kennedy@mayerbrown.com

[1] Article 13, SC Measures.

[2] The PIPL uses the term "personal information processor" (not to be confused with the commonly used term "data processor") to refer to "*organizations and individuals that, in personal information processing activities, autonomously decide processing purposes and processing methods*" – this is akin to the concept of a "data controller" under other commonly encountered data protection legislation.

[3] Article 4, SC Measures.

https://doi.org/10.1016/j.clsr.2023.105832
0267-3649

to be a possible practical solution. The revision ostensibly targets large companies seeking to carry out large data exports through the use of subsidiaries and related companies in a piecemeal fashion, in order to avoid the Security Assessment. Nevertheless, it is unclear in what circumstances a division of personal information would be prohibited and what would be considered *bona fide*.

1.1.4. *Obligations of data controllers*

Under the Standard Contract, data controllers are required to notify data subjects of the foreign recipient's name, contract information, purposes and methods of processing, types and retention period of personal information, the methods and procedures for exercising their rights as a data subject and "*other matters" (see Exhibit 1 (Instructions for the Export of Personal Information*").[4] Where the export involves sensitive personal information, the necessity and the impact of such export on the rights and interests of the data subjects must also be notified to them.

The primary basis for the collection and processing of personal information under the PIPL is the data subject's consent.[5] However, data controllers are required to obtain separate consent (e.g. unbundled consent) from data subjects in specific scenarios (e.g. export of personal information). The Standard Contract highlights one such scenario where separate, unbundled consent is required for the export of personal information, or from parents or guardians for the export of personal information of minors under the age of 14.[6]

Notably, data controllers must also inform data subjects of their third party beneficiary rights (see section on *Data Subject Rights* below), which crystalize if the data subject does not expressly object within 30 days.[7]

As the more "proximate" entity to the CAC, data controller exporters have the de facto burden of ensuring that the foreign recipient's data protection practices are sufficient; under the Standard Contract, data controllers have the burden of making "*reasonable efforts to ensure that the foreign recipient will take the necessary technical and management measures (encryption, anonymisation, de-identification, access control, and other technical and management measures)*".[8] Coupled with the added obligations of responding to inquiries from the Regulatory Authority regarding the processing activities of the foreign recipient,[9] and impact assessment to determine whether the foreign recipient's management, technical measures and capabilities to perform the responsibilities and obligations can ensure the security of exported personal information,[10] in effect this would mean a full audit of the practices of the foreign recipient pre-transfer. Such documentary evidence in practice will be gathered to satisfy the Personal Information Protection Impact Assessment ("**PIA**") requirements, and will need to be kept for at least 3 years.

Certification Specification V2.0 additionally requires entities applying for certification to be legal entities in the PRC that "*operate normally*" and maintain "*good reputation and goodwill*".[11]

1.1.5. *Strict compliance*

The SC Measures also now explicitly provide that the Standard Contract is to be used in its entirety, without deviation, unless otherwise directed by the CAC. In any event, while data controllers may include additional clauses in the Standard Contract (as an exhibit), such clauses should not conflict with the Standard Contract, which should prevail in any case.[12] Companies intending to export data out of the PRC should therefore re-visit their pre-existing documentation used for exporting data out of the PRC (e.g. intra-group data transfer agreements, data processing agreements etc.).

1.1.6. *PIA*

The SC Measures have retained the requirement for data controllers to carry out a PIA prior to the export of personal information. The PIA is to focus on the following areas:

1. The legality, legitimacy, and necessity of the purpose, scope, and methods of personal information processing by the data controller and foreign recipients;
2. The scale, scope, type, and sensitivity of exported personal information, and the potential risks to the rights and interests in personal information that may arise;
3. The responsibilities and obligations undertaken by the foreign recipient, as well as whether the management, technical measures and capabilities to perform the responsibilities and obligations can ensure the security of exported personal information;
4. The risk that personal information will be altered, destroyed, leaked, lost, transferred, or illegally acquired or used during or after export, and whether channels have been established to safeguard data subjects' rights and interests in their personal information rights;
5. The impact of the policies, laws, and regulations of the foreign recipient's jurisdiction on the performance of a standard contract; and
6. Other matters that may affect the security of personal information exported, and should be kept for at least 3 years.

Data controllers must submit the completed PIA report together with the executed Standard Contract to the regulatory authorities within 10 working days of the effective date of the Standard Contract,[13] though this appears to be a procedural formality without any need for regulatory approval, with data controllers being responsible for the "*veracity of documents filed*".[14]

These requirements are consistent with the PIA requirements under the other Security Assessment and Certification data export mechanisms.

[4] Article 2(2), Standard Contract.
[5] Article 13, PIPL.
[6] Article 2(3), Standard Contract.
[7] Article 2(4), Standard Contract.
[8] Article 2(5), Standard Contract.
[9] Article 2(7), Standard Contract.
[10] Article 2(8)(iii), Standard Contract.
[11] ibid.
[12] Article 6, SC Measures; Article 9(1), Standard Contract.
[13] Article 7, SC Measures.
[14] Article 8, SC Measures.

1.1.7. *Submission of documents*

The SC Measures have retained the requirement for data controllers to submit a new Standard Contract in certain circumstances though the first scenario has been narrowed slightly (dropping changes to the "quantity" and "retention period" of personal information). In such an event, the Standard Contract has to be executed again and filed anew with the regulatory authorities:

1. Changes to purpose, scope, type, sensitivity, methods, storage location of exported personal information, and the purposes and methods for which foreign recipients process data, or extend the period of overseas retention of personal information.
2. Changes to the policies, laws or regulations on the protection of personal information in the foreign recipient's jurisdiction that might impact rights and interests in personal information; or
3. Other circumstances that may impact rights and interests in personal information.

However, the SC Measures now allow data controllers to "*supplement [the Standard Contract]*" (i.e. file an addendum) as an alternative to re-filing the entire Standard Contract.

In practice most companies will opt for filing a supplement to the Standard Contract in the event of any of the changes detailed in the first scenario. The second and third scenarios remain tricky given the shifting sands of data protection regulations which will put the onus on data exporters to keep up to date with regulatory and legal changes and make an assessment whether such changes fall within the second scenario. The third scenario is nebulous and difficult to interpret and will likely never be invoked by data exporters but may prove a useful 'stick' for regulators especially if data exports are caught in the cross-fire of geopolitical battles.

The SC Measures now also require data controllers to carry out a new PIA to account for such changes in the scenarios outlined above and file the new PIA alongside the refreshed Standard Contract with the local CAC office. Data controllers should therefore be mindful as to changes to the circumstances in which it exports data since this could require it to prepare and file a new PIA and Standard Contract.

1.1.8. *Whistleblowing provision*

Violations of the SC Measures can be brought to the attention of the regulators by any third party (e.g. competitors and disgruntled former employees). Companies that export data out of the PRC should be mindful of this provision which highlights again the importance of compliance and of restricting sensitive discussions on data strategy to the C-suite and or personnel in management roles and on a "need to know" basis.

1.1.9. *Additional obligations for foreign recipients*

Under the finalized Standard Contract, there are also several new obligations for foreign recipients, including:

1. Obtaining separate consent of data subjects if any personal information is processed beyond the agreed purpose, method of processing and/or type of processing personal information.[15]
2. Obtaining separate consent from parents or other guardians of minors if personal information of a minor under the age of 14 is involved.[16]
3. (For data processor recipients) Returning or deleting personal information if the data processing agreement is ineffective, invalid, revoked or terminated, and providing a written statement to confirm such actions have been taken.[17]

The Draft Standard Contract previously required foreign recipients to take certain actions in the event of a "data breach". This has now been clarified to mean "*the occurrence or possible occurrence of alteration, destruction, leakage, loss, illegal use, unauthorized provision of or access to the processed personal information*".[18]

Under the SC Measures, where there has been a *possible* alteration, destruction, leakage, loss, illegal use, unauthorized provision of or access to the processed personal information, foreign recipients are required to:[19]

1. Take timely remedial action to mitigate adverse effects on data subjects;
2. Immediately notify the data controller and report to the regulatory authority as required by applicable laws, including the types of personal information affected, remedial actions taken, measures data subjects can take to mitigate damage, and the contact details of the personnel responsible for handling the breach; and
3. Document and retain all relevant evidence of alteration, destruction, leakage, loss, illegal use, unauthorized provision of or access to the personal information concerned, as well as of all remedial actions taken.

1.1.10. *Laws and regulations of the foreign recipient's jurisdiction*

The finalized Standard Contract requires both the foreign recipient and exporting data controller to warrant that they have "*exerted a reasonable duty of care*" when signing the Standard Contract, and they are not aware of personal information protection laws or regulations of the country where the foreign recipient is located, which include any provisions authorising public authorities to access personal information, that will impact a foreign recipient's performance of their obligations.[20]

This inclusion of "*reasonable duty of care*" is novel to the finalized Standard Contract, and while it is uncertain what this will entail, seems to suggest that a legal opinion of local counsel (of the foreign recipient jurisdiction) may be required – much like the Transfer Impact Assessments required under the GDPR in the wake of Schrems II.

Notably, this is not a blanket restriction on transfers to countries where public authorities may access personal infor-

[15] Article 3(1), SC Measures.
[16] ibid.
[17] Article 3(5), SC Measures.
[18] Article 3(7), SC Measures.
[19] ibid.
[20] Article 4(1), SC Measures.

mation, but appears to be a point for data controllers to analyse and assess. This is particularly in light of the new Article 4(6) of the Standard Contract, which requires foreign recipients to immediately notify the data controller in the event that it receives a request from a government department or judicial organ of the country in which it is located; data controllers may have to be wary of foreign jurisdictions that allow public authority access and prohibit notifications made to the exporting data controller. The provision mirrors somewhat data controller obligations under the PIPL[21] and Data Security Law ("**DSL**")[22] that prohibit the provision of personal information stored within mainland PRC to judicial or government bodies of foreign countries without the approval of the PRC regulatory authorities.

The Standard Contract allows a data controller to suspend and eventually terminate the contract in the event there are changes in the laws or mandatory measures in the country where the foreign recipient is located which makes it impossible for the foreign recipient to perform the contract. In short, any conflict of laws issue may result in the termination of the Standard Contract.

1.1.11. *Data subject rights*

Other than the data subject rights accorded to data subjects under the PIPL (e.g. access, restriction, correction, withdrawal of consent, portability, erasure etc.), under the finalized Standard Contract, data subjects are granted third party beneficiary rights that allow them to demand performance of various clauses of the Standard Contract[23] and take action for breach of the Standard Contract. In the event of a dispute, the data subject may lodge a complaint with the regulatory authority[24] or file a lawsuit with an appropriate people's court in accordance with the Civil Procedure Law of the PRC for a breach of the Standard Contract by either or both of the parties.[25]

Since such actions (i.e. complaints and/or a civil claim) will necessarily be premised on the information that is made available to the data subject, given the additional rights that data subjects in the PRC have (e.g. third party beneficiary rights,[26] right for data subject to obtain a copy of the SCC from both parties,[27] right for data subject to be informed of matters surrounding the export and processing of their personal information[28]), organisations engaged in exporting personal information from the PRC should be mindful of their communications and interactions with data subjects. Data controllers should ensure that they have necessary internal policies and procedures in place to allow them to respond to data subject requests in compliance with the law.

1.1.12. *Additional points of interest*

The ethos of the Standard Contract appears to be that of discouraging the export of personal information given the requirements for personal information to be exported to "the minimum extent required to achieve the purpose of processing"; or the emphasis on disclosure of the personal information to third parties only if there is a "real business need". This is further driven home by the manner in which the eligibility thresholds for the Standard Contract are framed i.e. "*personal information of less than 100,000 data subjects [counted from 1 Jan of the previous year]*", which point to exports of personal information being the exception rather than the norm since data controllers would have to have meticulous record-keeping practices should they wish to comply with the SC Measures.

Volume thresholds. Data controllers should note that the relevant date for determining whether a data controller falls within threshold 3 (i.e. data controllers who have exported personal information of fewer than 100,000 data subjects or sensitive personal information of fewer than 10,000 data subjects) is January 1 of the *previous year*.[29] Data controllers should therefore be mindful of the volume of personal information they export, particularly in the later part of the year (e.g. December) as this determines whether they are likely to be caught within this threshold, which essentially applies to the export of data for a period of up to 2 years. Where the personal information exceeds the stipulated thresholds in the SC Measures, or the data controller is a CIIO, the Security Assessment transfer mechanism 2 will apply. This will require data controllers to be very precise in their record keeping, and limit data exports on a "need to have" basis should they wish to avoid having to undergo a Security Assessment.

Scope of PIA and Exhibit 1 of the Standard Contract. Since changes to the purpose of processing and/or personal information storage location would necessitate a redo of both the PIA and Standard Contract, data controllers may wish to be prepare a more expansive PIA and Exhibit 1 (Instructions on the Export of Personal Information) of the Standard Contract.

Audit Rights. The foreign recipient has a broad obligation to provide the data controller with "all information necessary" to allow it to audit the compliance of processing activities.[30] This is accompanied by a corresponding obligation on the data controller provide all such information (including all compliance audit results) to the CAC as may be required by applicable laws.[31] Accordingly, data controllers engaged in pre-existing data transfers subject to pre-existing agreements should review this documentation to ensure that there are no additional impediments (which may not necessary conflict with the Standard Contract) that may nonetheless impair their ability to comply with the data controller obligations of the Standard Contract.

Unresolved issues. There are still outstanding questions on the practical applicability of the Standard Contract that remain unanswered, e.g. when would a division of personal data transfers be considered acceptable? How are data controllers exporting personal information expected to practically keep count of personal information exported, and what happens when a data export crosses the eligibility threshold that would require it to undertake a Security Assessment?

[21] Article 41, PIPL.
[22] Article 36, DSL.
[23] Article 5(5), 6(3), Standard Contract.
[24] Article 6(3)(i), Standard Contract.
[25] Article 6(5), Standard Contract.
[26] Article 5(5), Standard Contract.
[27] Article 2(9), 3(3), Standard Contract.
[28] Article 2(2), Standard Contract
[29] Article 4, SC Measures.
[30] Article 3(11), Standard Contract.
[31] Article 2(11), Standard Contract.

1.1.13. *Conclusion*

While the finalized Standard Contract sheds more light on the compliance requirements data exporters need to undertake, there are still outstanding practical issues that remain, and businesses with a presence in the PRC and those who deal with companies in the PRC ought to commence preparations to ensure they comply with the SC Measures by 30 November 2023.

Gabriela Kennedy *(Partner), Mayer Brown (*⟨13:italic ⟩gabriela.kennedy@mayerbrown.com⟨/13:italic⟩*); and* **Joshua Woo** *(Registered Foreign Lawyer (Singapore)), Mayer Brown (*⟨13:italic ⟩joshua.woo@mayerbrown.com⟨/13:italic⟩*).*

2. Hong Kong

2.1. *Trust in the crypto-verse: cryptocurrencies as a type of property in Hong Kong*

2.1.1. *Introduction*

The emergence of cryptocurrency as an investment asset, alongside the proliferation of blockchain technology has raised important legal questions, particularly regarding the legal status of cryptocurrency. Jurisdictions like Hong Kong have grappled with defining the legal nature of cryptocurrency, though a landmark decision has shed new light on the matter.

On 31 March 2023, Justice Linda Chan in *Re Gatecoin Limited* [2023] HKCFI 91 ("***Re Gatecoin***") held that cryptocurrency exhibits all the characteristics of property and could therefore be held on trust in the context of a liquidation (although it was ultimately found that the cryptocurrencies in question were not held on trust). In this article, we look at the key considerations underpinning the decision in *Re Gatecoin*.

2.1.2. *Salient facts*

Gatecoin Limited was a cryptocurrency exchange platform established in Hong Kong in 2015 which allowed customers to deposit, transfer and withdraw both cryptocurrencies and fiat currencies, and engage in cryptocurrency trading. Gatecoin itself was also engaged in cryptocurrency trading, including with its own customers. The company was wound up on 13 March 2019, and liquidators appointed on 20 March 2019. By 31 October 2022, over 50 types of cryptocurrencies valued at over HK$140 million were recovered by the liquidators. The liquidators contacted 102,600 creditors, though only 1,132 of them submitted their proof of debt. These creditors were customers with positive account balances on Gatecoin. It was acknowledged that the total value of the cryptocurrencies recovered by the liquidators would not be sufficient to fully reimburse all customers.

Three sets of Terms & Conditions ("**T&Cs**") were relevant to the case: the T&Cs effective:

- Between 28 January 2015 – November 2016 ("**2016 T&Cs**");
- From November 2016 – March 2018 ("**Trust T&Cs**"); and
- From 6 March 2018 – 13 March 2018 ("**2018 T&Cs**").

Customers who signed up with the platform during the period when the 2016 T&Cs were in effect were referred to as "Group A." Those who signed up when the Trust T&Cs were in place were known as "Group B," while customers who agreed to the 2018 T&Cs were classified as "Group C."

While the 2016 T&Cs did not include provisions to the effect of creating a trust, Gatecoin reserved the right to modify the terms "*without prior notice*" to customers. In November 2016, Gatecoin introduced the Trust T&Cs, which explicitly stated that customers would have a beneficial ownership interest in the digital assets, and Gatecoin would act as a custodian holding the digital assets in trust. Gatecoin was also obligated to inform customers *before* making material changes to the terms, and customers were asked to agree to these changes. Starting from 6 March 2018, and continuing until the winding-up order, Gatecoin adopted the 2018 T&Cs, which stated that Gatecoin was not a fiduciary, and customers should not expect to receive additional cryptocurrencies created by any blockchain forks.

2.1.3. *Cryptocurrency as property*

The first key question was whether the liquidators even had the authority to realize and distribute the cryptocurrencies in the winding-up process. While Section 197 of the *Companies (Winding Up and Miscellaneous Provisions) Ordinance* (Cap. 32) ("**CWUMPO**") stipulates that liquidators must take custody of all "property" upon a winding-up order, "property" is not defined in the CWUMPO. Accordingly, it was necessary for the court to examine the statutory definition of "property" pursuant to Section 3 of the *Interpretation and General Clauses Ordinance* (Cap. 1) as well as the criteria outlined by Lord Wilberforce in *National Provincial Bank v Ainsworth* [1965] 1 AC 1175 ("***Ainsworth***"), which include being "*definable, identifiable by third parties, capable in its nature of assumption by third parties, and having some degree of permanence or stability*."

The court also reviewed the approach taken by common law jurisdictions such as England and Wales, the British Virgin Islands, Singapore, Canada, the United States, Australia, and New Zealand. She particularly relied on the New Zealand High Court decision of *Ruscoe v Cryptopia* [2020] NZHC 728 ("***Ruscoe***"), which shared similar facts with the present case.

In *Ruscoe*, liquidators of a cryptocurrency trading exchange sought directions from the court regarding the nature of cryptocurrency and whether it could be subject to a trust. The court in *Ruscoe*, concluded that a cryptoasset is a form of property after considering the criteria discussed in *Ainsworth*.

Justice Chan agreed with the analysis in *Ruscoe*, and held that the definition of property is broad enough to include cryptocurrency, even if it cannot be strictly classified as either a *chose in possession* or a *chose in action*.

In particular, the court relied on the following reasoning in reaching its decision (at [57]):

(1) *"It is definable as the public key allocated to a cryptocurrency wallet is readily identifiable, sufficiently distinct and capable of being allocated uniquely to individual accountholder (§§104–108).*
(2) *It is identifiable by third parties in that only the holder of a private key is able to access and transfer the cryptocurrency from one wallet to another (§§109–113).*
(3) *It is capable of assumption by third parties in that it can be and is the subject of active trading markets where (a) the*

rights of the owner in that property are respected, and (b) it is potentially desirable to third parties such that they want themselves to obtain ownership of it (§§114–116).

(4) *It has some degree of permanence or stability as the entire life history of a cryptocurrency is available in the blockchain (§§117–119)", therefore concluding that cryptocurrencies were a form of property that could be held on trust.*

2.1.4. *Construction of terms & conditions*

Notwithstanding the court's determination that cryptocurrencies could be held on trust, the second question was whether Gatecoin had in fact held the cryptocurrencies on trust for its customers, giving customers a proprietary claim over the cryptocurrencies.

Whether a trust has been created turns on whether the "three certainties" have been fulfilled – subject matter, object and intention.

The court found that there was certainty of subject matter by likening cryptocurrencies to shares where the absence of a beneficiary's ability to appropriate a specific part of the fungible mass would not invalidate a trust as long as the proportionate share of the beneficiary is able to be clearly demarcated, such as a ledger used to record a customer's corresponding contribution. Similarly, the court found that certainty of object was similarly fulfilled by the same ledger which recorded the list of beneficiaries and their claim over the trust assets.

The biggest issue lay with the certainty of intention, and whether the 2018 T&Cs, which expressly disclaimed a trust arrangement, applied.

The liquidators argued that both the assets in the accounts of Group A and B customers were held on trust since:

- The Trust T&Cs superseded the 2016 T&Cs that Group A customers had agreed to, and hence applied in place of the 2016 T&Cs;
- Group B customers opened their accounts when the Trust T&Cs were in effect;
- The digital assets of Group A and Group B customers were considered trust property when the Trust T&Cs were in effect;
- The Trust T&Cs explicitly stated that customers would have a beneficial ownership interest in the digital assets; and
- Gatecoin was obligated under the "Trust T&Cs" to inform customers *before* making material changes to the terms, but Gatecoin failed to do so before it implemented the 2018 T&Cs.

However, the court focused on the intention of the parties as "*ascertained by an objective assessment of the terms of the agreement or relationship (between the parties) with reference to that property*," and found that both Group A and Group B customers must have agreed to the 2018 T&Cs in order to continue their access to the Gatecoin platform. Accordingly, the court held that the "*contractual bargain reached between the parties*" (i.e. 2018 T&Cs) should not ignored, and that Group A and B customers should not be allowed to rely on the terms of the Trust T&Cs.

In essence, all three groups of customers, save for those who did not access or use the platform during the period when the 2018 T&Cs were implemented up to the date of liquidation, were therefore governed by the 2018 T&Cs. Since the 2018 T&Cs expressly disclaimed a trust arrangement, Group A, B, and C customers were only found to have contractual claims against Gatecoin.

2.1.5. *Comments and takeaways*

The case highlights the attempt by Hong Kong courts to fit cryptocurrencies into the framework of traditional property law through the application of existing legal principles. Although cryptocurrencies may not fit neatly within the traditional classification of "property," they possess characteristics of intangible property similar to stocks and shares, which was reflected in their treatment in *Re Gatecoin*.

Additionally, the case demonstrates the court's willingness to recognize cryptocurrency exchange platforms as trustees, and impose fiduciary duties on them. This development aligns with the recent recommendations by the Hong Kong Securities and Futures Commission for virtual asset exchanges to protect client assets by holding them on trust, and to separate these assets from their own property. Platform users, potential investors of cryptocurrency platforms, and cryptocurrency platform operators should therefore take note of how the Terms & Conditions of the cryptocurrency platforms are drafted and carefully consider the ramifications on their rights in relation to cryptocurrencies held by the platform or debts owed by the platform.

Furthermore, while not directly in issue, the court, in finding that the Group A and Group B customers had accepted the 2018 T&Cs by "*click[ing] to acknowledge and accept the 2018 T&C before they could continue to access and use [the Platform]*", affirmed the enforceability of clickwrap contracts in Hong Kong.

Re Gatecoin has provided valuable clarity on the legal status of cryptocurrency as property, and the implications for trust arrangements surrounding cryptocurrencies. The case sheds light on the evolving legal landscape surrounding cryptocurrencies, and sets a precedent for future cases in Hong Kong and beyond.

The authors would like to thank Sabrina Chow, Trainee Solicitor at Mayer Brown, for her assistance with this legal update.

Gabriela Kennedy *(Partner), Mayer Brown* (⟨13:italic ⟩gabriela.kennedy@mayerbrown.com⟨/13:italic⟩); *and* **Joshua Woo** *(Registered Foreign Lawyer (Singapore)), Mayer Brown* (⟨13:italic ⟩joshua.woo@mayerbrown.com⟨/13:italic⟩).

3. Japan

3.1. *Legal reforms to restrict counterfeit products on the Metaverse*

3.1.1. *Introduction*

The Metaverse is currently the centre of attention for many trademark practitioners and we are seeing increasing amounts of litigation centred on the digital space, such as the MetaBirkins case and *Nike v. StockX*. There are also many discussions on how brand owners can protect trademarks in

the digital space and what classes, goods/services and countries/regions should be considered when filing trademarks to protect those activities in the Metaverse.

In order to prevent acts of imitation in the digital space, the Japanese Cabinet approved an amendment ("**Amendment**") to the Unfair Competition Prevention Act ("**Act**") and submitted to the Japanese Diet on 10 March 2023. The Japanese Diet is likely to pass the Amendment by this June. The Amendment is to broaden the "acts of unfair competition" prohibited under the Act to those done in the digital space.

3.1.2. *Amendment*

Section 2, Paragraph 1, Item 3 of the current Act defines the transfer of products that have the same or substantially similar forms (designs) as those of others ("**Imitations**") as an "act of unfair competition". This provision can only be used against imitators by sellers of new original products, namely for original products within 3 years from the launch of the product in Japan.

The Amendment to this provision adds "offe*ring (of Imitations) through a telecommunication line*" to the other acts such as transferring, exhibiting, exporting and importing of the Imitations.

Under the current Act, only a "*transfer of physical products*" is prohibited, and only tangible products are subject to this provision. Therefore, offering digital data (intangible property) such as images or videos that resemble the original product would not found to be an "act of unfair competition" under the current Act. This would allow people to sell digital data that is an imitation of another person's original product.

The Amendment to the provision was introduced to deal with such cases. Because it is foreseeable that more and more activities and transactions will be made in the Metaverse, it would result in unfair outcomes if no action can be taken against parties who make money by free-riding on other parties' designs in the digital space.

In discussing the Amendment, the government study committee ("**Committee**") also discussed the pros and cons of extending the protection period of 3 years when the sale and offer of Imitations is prohibited. However, the Committee was divided between those in favour and those opposed to extending the period, and decided to continue the discussion.

The protection of virtual objects by design rights was also discussed by the Committee. Concerned about the effect of discouraging creators' creative activities, the Committee decided not to revise the Design Act on the grounds that such a revision should be carefully considered.

3.1.3. *Future movement*

The Amendment itself is a small step and it is only limited to imitation of designs of new products. However, it is a good sign that the Japanese Government is taking infringement in the digital world as a serious matter. In the digital space, the unauthorised creation and use of avatars that imitate the likeness of real people, as well as impersonation and defrauding of other persons' avatars, have become a problem, and the Committee is also considering whether protection can be provided by the rights of publicity and likeness. We expect to see more rule making concerning issues in the digital space after discussions with the relevant sectors.

Kiyoko Nakaoka *(Partner), Kubota* (⟨13:italic ⟩nakaoka@kubota-law.com⟨/13:italic⟩).

4. Singapore

4.1. *Singapore high court finds employer vicariously liable for copyright infringement due to Employee's infringing acts*

In *Siemens Industry Software Inc. (formerly known as Siemens Product Lifecycle Management Software Inc) v Inzign Pte Ltd* [2023] SGHC 50, the Singapore High Court ("**SGHC**") held that an employer was vicariously liable for copyright infringement on account of its employee's acts, despite being unaware of the same.

4.1.1. *Background facts*

Siemens Industry Software Inc. (the "**Plaintiff**") was the copyright owner of NX Software, a commercial and industrial software used for computer-aided design, manufacturing and engineering. The NX Software comprises of multiple modules with varying functionalities, and users will typically purchase licenses for modules specifically applicable to their respective businesses.

Inzign Pte Ltd (the "**Defendant**") held licenses to three modules of the NX Software. The software was used by the Defendant's machinist, Mr Paing Win (the "**Employee**"), in the course of his work.

After coming across instructions on how to install a full version of the NX Software online, the Employee installed an unauthorised full version of the NX Software on an unused and unsecured laptop which he found in a toolroom at the Defendant's premises.

The Plaintiff became aware of the unauthorised installation via an automatic reporting function built into the software, and subsequently informed the Defendant of the same. Thereafter, the Defendant conducted an internal investigation and uninstalled the software in question.

The Plaintiff eventually commenced proceedings against the Defendant for copyright infringement, and sought to argue that the Defendant was both primarily and vicariously liable for the Employee's infringing acts.

4.1.2. *Decision*

The SGHC found that the Defendant was not primarily liable for copyright infringement, but reached a different conclusion in respect of vicarious liability.

In particular, the SGHC held that the doctrine of vicarious liability could extend to copyright infringement, and applied the following legal test:

(a) there must be a special relationship between the Employee and the Defendant; and
(b) there must be sufficient connection between the Defendant and the Employee on the one hand, and the commission of the infringing acts on the other.

In the present case, the contractual employment relationship between the Defendant and the Employee was sufficient to satisfy the requirement under limb (a).

In respect of limb (b), the SGHC held that a sufficient connection existed between the Employee's employment with the Defendant and the infringing acts for the following reasons:

(a) the circumstances in which the Employee was allowed to operate in the course of his work afforded him the opportunity to commit the infringing acts, particularly the Defendant's lax supervision of the Employee and failure to take reasonable steps to prevent the infringing acts;
(b) the Defendant's mismanagement of the laptop, such as the toolroom manager's failure to properly secure the laptop in the toolroom and inform the Defendant of its existence, also facilitated the infringing acts; and
(c) the infringing acts were committed in the context of the Employee's employment and for the Defendant's benefit—the Employee had installed the unauthorised version of the NX Software so that he could practise using it to improve his performance at work.

The SGHC also cited the following policy considerations in support of its finding of vicarious liability:

(a) the imposition of vicarious liability on the Defendant will ensure the effective compensation of the Plaintiff as it is best placed and most able to provide such compensation; and
(b) a finding of vicarious liability in this case will incentivise employers to take further steps in reducing the incidence of copyright infringement by their employees.

4.1.3. *Comment*

This decision establishes that the doctrine of vicarious liability applies to copyright infringement in Singapore law. Notably, it also demonstrates that employers may be at risk of being held vicariously liable for acts of copyright infringement committed by their employees under some circumstances. Employers should be vigilant in enforcing their anti-piracy policies as well as exercise adequate supervision and control over their employee's actions.

4.2. *Singapore high court rules that a debt in cryptocurrency is not a money debt*

According to section 125(1)(e) read with section 125(2)(a) of the Insolvency, Restructuring and Dissolution Act 2018 ("**IRDA**"), a winding-up application can be brought by a creditor to whom a company is indebted in a sum exceeding S$15,000 if:

(a) the creditor has served a statutory demand on the company requiring that it pay the sum due; and
(b) the company fails to, amongst other things, pay the sum within three weeks.

In an unreported decision of the SGHC in *Algorand Foundation Ltd v Three Arrows Capital Pte Ltd*, the SGHC held that a debt denominated in cryptocurrency is not a money debt in the context of a winding-up application.

4.2.1. *Background facts*

Algorand Foundation Ltd (the "**Applicant**"), a blockchain company, commenced proceedings to seek a winding up order against the Singapore entity of a cryptocurrency fund, Three Arrows Capital Pte Ltd (the "**Defendant**"). The basis of their application was an alleged unsatisfied liability of 53.5 million USD Coin ("**USDC**"), a type of stablecoin cryptocurrency pegged to the US dollar.

4.2.2. *Decision*

The SGHC dismissed the winding-up application and found that a debt denominated in cryptocurrency would not be considered a debt for a sum of money for the purposes of the IRDA. In this regard, the SGHC expressed the view that the word "indebtedness" must require a debt which is in fiat currency.

Accordingly, it was held that while the Applicant had standing to bring a winding-up application as a creditor, it did not possess a claim for a money debt. As a result, the statutory demand, which was for a debt denominated in cryptocurrency, was invalid for the purposes of establishing a basis for a winding-up application under section 125(1)(e) and section 125(2)(a) of the IRDA.

In delivering its decision, the SGHC also highlighted that the determination of whether or not a particular intangible, such as cryptocurrency, is money would require a detailed examination of evidence which is not appropriate in the context of insolvency.

4.2.3. *Comment*

This decision addresses, for the first time, the question of whether a cryptocurrency debt would be considered a debt for a sum of money in the context of winding-up proceedings. Whether cryptocurrency will be considered a form of money under Singapore law remains an open issue, but this case merits attention as one of the first judicial determinations as to the status of cryptocurrencies.

Lam Chung Nian *(Partner), WongPartnership LLP (*⟨13:italic ⟩chungnian.lam@wongpartnership.com⟨/13:italic⟩*); and* **Megan Low** *(Associate), WongPartnership LLP (*⟨13:italic ⟩megan.low@wongpartnership.com⟨/13:italic⟩*).*

5. South Korea

5.1. *Second major amendment to the Personal Information Protection Act passed by National Assembly*

5.1.1. *Introduction*

On 27 February 2023 the National Assembly passed a bill containing a number of amendments to the Personal Information Protection Act (the "**Amended PIPA**"), Korea's general data protection law. The Amended PIPA, which represents the second step of the Korean government's multi-step amendment process for the PIPA following the passage of the first amendment in 2020, is scheduled to go into effect 6 months from its promulgation date (which must take place within the next 15 days). However, certain provisions therein, including those relating to automated decision-making and the right to data portability, are scheduled to go into effect 12 months thereafter.

The legislative purpose of the Amended PIPA is to facilitate the use of personal information while strengthening the protection of data subjects' rights and ensuring compatibility

and interoperability with the global regulatory regime in the advent of the digital economy.

The amended PIPA, albeit partial, contains major substantive changes that may have a serious impact on companies' data protection and privacy policies. The following is a summary of the key changes introduced by the amendments.

5.1.2. *Provisions relating to the processing of personal information in general*

5.1.2.1. *Unification of data protection rules for offline and online businesses* The current PIPA prescribes one set of data protection rules for ordinary data controllers (a concept similar to that of a "data controller" under GDPR) and a different set of data protection rules for data controllers that are information communications service providers (or "**ICSPs**", a concept which is interpreted quite broadly to include providers of a wide range of services offered over telecommunications or information services networks). The Amended PIPA eliminates this discrepancy by subjecting ordinary data controllers and ICSPs to the same data protection rules and requirements based on the principle of the "same regulation of the same act." Accordingly, Chapter 6 (Articles 39-3 to 39-15) of the current PIPA, which applies only to ICSPs, is deleted in its entirety under the Amended PIPA. However, certain special rules applicable only to ICSPs (i.e., some of the deleted provisions) have been (i) consolidated with other general provisions overlapping substantially therewith or (ii) expanded in scope for application to all data controllers after being moved elsewhere under the Amended PIPA.

The aforesaid unification of data protection rules are expected to address persistent criticism that the different data protection rules under the current PIPA, applying respectively to ordinary data controllers and ICSPs, create unnecessary confusion in regards to enforcement because the distinction between the two is not always clear. These latest changes, however, may increase the compliance burden of offline businesses which will become subject to additional data privacy requirements under the Amended PIPA which currently apply only to ICSPs. Thus, offline businesses are advised to closely follow corresponding amendments to the Enforcement Decree of the PIPA to check if and to what extent they may be subject to such additional data privacy requirements.

5.1.2.2. *Revamping of provisions relating to administrative penalties and criminal penalties (Articles 64-2 and 71 ~ 73)* The Amended PIPA also seeks to revamp some of the administrative penalty and criminal penalty provisions as follows.

5.1.2.2.1. *Consolidation of administrative penalty provisions* Under the current PIPA, different provisions prescribe administrative penalties for various violations ranging from (i) unlawful processing of pseudonymized information, (ii) leakage of resident registration numbers, and (iii) violations committed specifically by ICSPs, such as failures to obtain consent. Under the **Amended PIPA, however, all administrative penalties will be prescribed by a single provision – the newly created Article 64-2 – which will apply to both ordinary data controllers and ICSPs alike.**

Offline businesses are advised to take note that the collection/use of personal information without consent and the collection/use of personal information of a data subject under 14 without his/her legal representative's consent will be subject to an administrative penalty under the Amended PIPA instead of an administrative fine under the current PIPA.

5.1.2.2.2. *Changing the upper limit of administrative penalties* Under the current PIPA, the upper limit of the administrative penalty **is 3% of the sales revenue** related to the activity in violation of the PIPA. Under the Amended PIPA, however, the upper limit of the administrative penalty will, in principal, be 3% of total sales revenue unless the data controller can successfully argue for the exclusion of any sales revenue unrelated to the activity in violation of the PIPA.[32] However, it should be noted that **if a data controller refuses to submit sales calculation data without a justifiable reason or submits any such data that is false, the upper limit of the penalty may be calculated based just on 3% of total sales revenue, with the inclusion of sales revenue that appears unrelated** to the activity in violation of the PIPA.

5.1.2.2.3. *Revamping of criminal penalty provisions* The Amended PIPA will prescribe the same criminal penalties for the same violations irrespective of whether such violations are committed by ordinary data controllers or ICSPs. However, certain violations which are currently subject to criminal penalties will be subject only to administrative penalties under the Amended PIPA. Specifically, provisions in the current PIPA prescribing criminal penalties for (i) the leakage of personal information due to the data controller's failure to implement mandatory security measures, (ii) an ICSP's collection and use of personal information without consent, and (iii) a failure to destroy personal information have been deleted from the Amended PIPA.

5.1.2.3. *Easing of consent requirements for the processing of personal information* The Amended PIPA will ease certain requirements for the processing of personal information without the data subject's consent as below.

1. The current PIPA provides that personal information may be collected and used without the data subject's consent in cases where such collection/use is "unavoidably necessary" for entering into and performing a contract with such data subject. However, the phrase "unavoidably necessary" will be deleted from the relevant provision (Art. 15(1)(iv)) in the Amended PIPA, thereby reducing the excessive reliance on the data subject's consent as a legal base for the collection/use of personal information.
2. In addition, the current PIPA provides that personal information may be used/provided beyond consented purposes if there exists a clear and urgent need to protect the life, physical body or economic interest of the data subject or a third party, and consent for such use/provision cannot be obtained because the data subject or his/her legal representative is unable to express his/her intent or his/her address is unknown. However, the phrase "and consent for such use/provision cannot be obtained because

[32] Initially, the Government Proposal only stated a maximum administrative penalty amount of 3% of total sales revenue, which was subsequently changed, after the public commentary period, to permit the exclusion of any sales revenue unrelated to the activity in violation of the PIPA.

the data subject or his/her legal representative is unable to express his/her intent or his/her address is unknown" will be deleted from the relevant provision (Art. 18(2)(iii)) in the Amended PIPA, thereby easing requirements for the use/provision of personal information without consent in cases where there is an urgent need to protect the lives of individuals.
3. Lastly, the Amended PIPA will contain newly created provisions (Art. 15(1)(vii) and Art. 18(2)(x)) that will permit the collection/use of personal information without consent and the collection/provision of personal information beyond consented purposes if urgently necessary to ensure public safety and well-being, including public health (e.g. prevention of the spread of COVID-19 and other infectious diseases).

5.1.2.4. *Revamping of provisions relating to the mediation of disputes involving personal information* To promote the mediation of disputes involving personal information by the Personal Information Dispute Mediation Committee (the "**PIDMC**") as a more efficient alternative to litigation for the settlement of such disputes, the Amended PIPA will amend or newly create several provisions such as the following:

1. The scope of data controllers obligated to participate in mediation by the PIDMC (Art. 43(3)) has been expanded from public institutions (under the current PIPA) to data controllers in general.
2. Committee members of the PIDMC and public officials belonging to related organizations will be granted new authority to conduct relevant fact-finding by visiting locations related to the dispute to conduct investigations and view relevant materials (Art. 45(2),(3)).

Consequently, it is anticipated that data subjects will be able to exercise their rights more robustly than before by taking advantage of these improvements which, in turn, is expected to result in more dispute mediation cases before the PIDMC and a corresponding increase in the burden of data controllers to respond to such cases.

5.1.2.5. *Other amendments* Notably, the Amended PIPA will also contain, amongst others, the following provisions relating to the processing of personal information:

1. If a data controller determines that there is a risk of privacy infringement due to the inclusion of sensitive information in the information that will be disclosed in the course of providing goods/services, such data controller will be required to provide data subjects with prior notice of (i) the possibility that their sensitive information may be disclosed and (ii) the methods on how to choose not to disclose their sensitive information (Art. 23(3)).
2. New obligation imposed on data controllers to destroy pseudonymized information in their possession (Art. 28-7).
3. An evaluation system for privacy policies will be introduced which will allow them to be assessed for compliance with applicable requirements, including whether privacy policies have been prepared/disclosed in a manner easily understandable /viewable by data subjects, and provide for the recommendation of improvements (Art. 30-2).
4. The Personal Information Protection Committee ("**PIPC**") will be granted discretion to specially reduce or waive any administrative fines it has imposed after considering extenuating circumstances such as the severity/motivation/results of the activity in violation of the PIPA and the scale of the data controller's business operations (proviso to Art.75(5)).

5.1.3. *Provisions relating to the processing of special categories of personal information*

5.1.3.1. *Revamping of provisions relating to visual information processing devices* The current PIPA only regulates "stationary" visual information processing devices such as CCTVs. In contrast, the Amended PIPA will introduce new provisions to regulate "mobile" visual information processing devices (e.g. drones, autonomous vehicles) while revamping existing provisions on the regulation of stationary visual information processing devices as below.

5.1.3.1.1. Introduction of new provisions for mobile visual information processing devices Under the current PIPA, the use of mobile visual information processing devices to film or photograph data subjects in open spaces for business purposes is permitted when doing so pursuant to legal bases such as data subjects' consent or the data controller's legitimate interest. The Amended PIPA will additionally permit the use of mobile visual information processing devices for such filming/photographing in cases where (i) data subjects **have refrained from indicating their refusal thereof** despite being clearly aware of such filming/ photographing taking place **as indicated by light, sound, or signboards** and (ii) such filming/photographing is conducted only to a reasonable extent and is unlikely to unfairly infringe the rights of data subjects (Art. 25–2).

This new provision is noteworthy because it alleviates the difficulty of the filming/photographing party, under the current PIPA, of having to obtain opt-in consent from a large number of unspecified individuals **or** identify its legitimate interest when using mobile visual information processing devices to film/photograph their personal information.

However, there is some uncertainty as to whether it will be possible for data subjects, who do not wish to be filmed/photographed by such mobile visual information processing devices, to adequately express their refusal in accordance with this statutory mechanism. Therefore, to obtain a greater level of clarity, it will be necessary to closely follow how the PIPC will interpret and enforce this provision in the future.

5.1.3.1.2. Revamping of existing provisions for stationary visual information processing devices Under the current PIPA, the filming or photographing of data subjects using stationary visual information processing devices is only permitted when such devices are installed in open spaces for certain legally prescribed purposes such as facility safety, fire prevention, and traffic control. The Amended PIPA will additionally permit the use of stationary visual information processing devices in open spaces for certain other purposes (to be specified by corresponding amendments to the Enforcement Decree of the PIPA) provided that no storage of the

filmed/photographed personal information takes place. However, regarding the aforementioned purposes related to facility safety, fire prevention, and traffic control, the Amended PIPA will additionally require that the stationary visual information processing devices be installed/operated only by "**persons who are duly authorized**" to conduct activity necessary to achieve such purposes (Art. 25(1)).

5.1.3.2. *Introduction of rights relating to automated decision-making* Under the Amended PIPA, data subjects will have the following rights in relation to automated decision making (Art. 37-2)[33]:

1. The right to request an explanation from the data controller in cases where they have been subjected to automated decision-making.
2. The right not to be subject to automated decision-making in certain cases when automated decision-making is likely to affect/has affected their rights or obligations significantly, except when such decision-making is made on the basis of data subjects' consent, legal provisions or the need for the execution/performance of a contract between the data subjects and the data controller.

Upon the exercise of the aforementioned rights by a data subject the data controller will be required to, unless there is a justifiable reason not to, take necessary measures such as excluding the data subject from automated decision-making, re-processing his/her personal information with human involvement or providing an explanation thereon. The data controller is also required to take certain other measures, such as disclosing the criteria and procedures for automated decision-making in a manner easily noticeable by data subjects.

Similar rights relating to automated decision-making have already been introduced in the GDPR and the Credit Information Use and Protection Act of Korea (the "**Credit Information Act**"). However, the rights prescribed by the GDPR and the Credit Information Act differ in certain respects to those prescribed by the Amended PIPA. Specifically, the GDPR only prescribes the data subject's right to refuse/object to a decision and the right to express his/her point of view (Art. 22(3)) while the Credit Information Act only prescribes the data subject's right to request an explanation, the right to submit information, and the right to object to a decision in certain cases (Art. 36-2(1), (2)).

The introduction of the aforementioned rights related to automated decision-making in the Amended PIPA can be seen as a meaningful measure to prevent the infringement of the rights data subjects at a time when data controllers are relying increasingly on automated decision-making due to rapid advances in artificial intelligence technology.

[33] Decisions made automatically and without human intervention after processing personal information entirely by automated systems, such as those using artificial intelligence technology (Art.4(vi)).

5.1.3.3. *New rules for cross-border transfers of personal information*

5.1.3.3.1. *Expansion of legal bases for cross-border transfers of personal information* Under the Amended PIPA, the legal bases pursuant to which personal information may be transferred cross-border have been expanded to include the following (Art. 28-8):

1. When the data subject has separately given his or her **consent**;
2. When there are special provisions regarding the cross-border transfer of personal information in **laws, treaties, or international agreements**;
3. When the (i) outsourcing of the processing of personal information or the storage thereof is **necessary for the execution or performance of a contract** and (ii) information[34] that must be notified to data subjects when obtaining consent for the cross-border transfer of personal information has been **disclosed in the privacy policy or notified individually to data subjects** via methods prescribed by the Enforcement Decree of the PIPA (e.g. by email);
4. If the overseas recipient has obtained data protection certification prescribed by the PIPC and has taken all of the following measures:
   a. security measures necessary for the protection of personal information and measures necessary to guarantee the rights of data subjects; and
   b. measures necessary to conduct data processing in accordance with data protection certification in the country where personal information is to be transferred; and
5. When personal information will be transferred cross-border to a country or international organization recognized by the PIPC as having essentially equivalent levels of data protection as those required under the PIPA.

5.1.3.3.2. *Orders to cease the cross-border transfer of personal information (Art. 28-9)* Under the Amended PIPA, the PIPC will be newly authorized to order[35] data controllers to cease cross-border transfers of personal information in cases where: (i) such cross-border transfers are taking place or expected to take place in a manner that violates the PIPA; or (ii) the recipient, country, or international organization receiving the personal information is not adequately (vis-à-vis what is required under the PIPA) protecting personal information and data subjects are being harmed or likely to be harmed as a result (Art. 28-9). A failure to comply with the PIPC's order to cease the cross-border transfer of personal information may result in an administrative penalty of up to 3% of total sales revenue (less any sales revenue unrelated to the activity in violation of the PIPA) (Art. 64-2(vii), (viii)).

[34] Under the Amended PIPA, information on the "methods and procedures for refusing the transfer of personal information and the effects thereof" must also be notified to data subjects when obtaining consent for cross-border transfers of personal information.

[35] Data controllers that have been ordered by the PIPC to cease the cross-border transfer of personal information as above will have an opportunity to file an objection within seven (7) days from the receipt of the order.

These latest amendments reflect and take into account the growing demand for cross-border transfers of personal information by expanding the legal bases for such transfers to take place. Also, by granting authority to impose orders to cease cross-border transfers, the Amended PIPA will bestow upon the PIPC powers similar to those enjoyed by regulatory authorities under the GDPR (Art. 58(2)(j)). It should be noted, however, that, unlike the GDPR, the Amended PIPA does not specify standard contractual clauses or binding corporate rules as legal bases for a cross-border transfer. Accordingly, companies that are transferring personal information overseas from Korea will need to be mindful of these new rules governing cross-border transfers to avoid the risk of a cessation order or other sanctions from the PIPC.

5.1.4. *Provisions relating to the right to data portability*

5.1.4.1. *Establishment of new provisions relating to the right to data portability* The Amended PIPA contains a new provision (Art. 35-2), which will go into effect on a to-be-determined date between 12 months and 24 months after its 14 March 2023 promulgation date, that grants data subjects the right to request transmission of their personal information to either themselves or third parties so long as such personal information is not generated from analysis/processing of the same collected by the data controller and meets the following criteria:

1. the personal information must have been (i) processed based on the consent of the data subject; (ii) processed to perform a contract executed with the data subject or to implement measures requested by the data subject in the course of executing the contract; or (iii) designated by the PIPC pursuant to a request from a central administrative agency for the data subject's or public interest in cases where the transmission thereof is permitted by or unavoidably necessary for compliance with law; is unavoidably necessary for a public institution to conduct its statutorily prescribed tasks; or concerns sensitive information or unique identification information and its processing is permitted or required by law; and
2. the personal information must have been processed by an information processing device such as a computer.

Upon request from a data subject, the data controller must transmit the personal information in a commonly used and machine-readable format, which can be processed through a data processing device (e.g. computer), to the extent technically feasible and reasonable in terms of time and cost. In addition, the PIPC will be authorized to create a personal information transmission support platform that will provide data subjects with certain information (e.g. items of personal information that can be transmitted, records of transmission requests/withdrawals made by data subjects) necessary for the transmission of their personal information. In case of requests for transmission to a third party, the third party must be a professional institution specialized in personal information management ("**Specialized Institution**") or another data controller that has implemented the requisite technical, managerial, and physical security measures and has satisfied relevant standards for facilities/equipment prescribed by the PIPA and its Enforcement Decree.

Further, the Amended PIPA contains an additional provision (Art. 35-3), scheduled to go into effect one year after its 14 March 2023 promulgation date, that will obligate organizations to receive designation as a Specialized Institution from the PIPC or the relevant central administrative agency when seeking to conduct any of the following tasks: (i) support data subjects with the exercise of their right to data portability; (ii) establish/standardize a personal information transmission system or manage/ analyse personal information to support data subjects with the exercise of their rights; or (iii) any other tasks prescribed by the Enforcement Decree of the PIPA to effectively support data subjects with the exercise of their rights.

It is anticipated that forthcoming amendments to the Enforcement Decree of the PIPA will include further details of, amongst other things, the criteria for personal information which may be the subject of a transmission request, standards for determining which data controllers would be subject to the data subjects' right to data portability, methods of requesting transmission, and the methods of transmission/transmission refusal/transmission suspension.

5.1.4.2. *Implications* The introduction of the right to data portability is intended to further strengthen the data subject's control over his/her own personal information across all sectors where it is processed alleviate the monopolization of the processing of personal information by the major platform operators, and lay the groundwork for various economic entities, such as start-ups, to safely utilize personal information. Although there are differing views on what the actual impact of the right to data portability may be, the introduction of this right is likely to bring about significant changes in the way personal information is processed in Korea.

However, data standardization will be essential to facilitating the transmission of personal information between companies and across industries, and judging from precedents in the financial sector where a similar right to data portability was introduced previously in August 2020, this task is expected to pose considerable technical and economic challenges.

Furthermore, because the right to data portability under the Amended PIPA was designed to not only enhance the rights of data subjects but also to facilitate the data economy, this right differs to its namesake under the GDPR whose focus is mainly on the protection of data subjects and thus, the former may need to be interpreted differently from the latter in certain respects. Therefore, due to this degree of uncertainty regarding how the interpretation and application of this PIPA right may take shape in the future, companies are advised to closely follow corresponding amendments to the Enforcement Decree of the PIPA and other regulations issued thereunder.

Kwang Bae Park *(Partner), Lee & Ko* (⟨13:italic ⟩kwangbae.park@leeko.com⟨/13:italic⟩); **Jongsoo (Jay) Yoon** *(Partner), Lee & Ko* (⟨13:italic ⟩jay.yoon@leeko.com⟨/13:italic⟩); **Hwan Kyoung Ko** *(Parnter), Lee & Ko* (⟨13:italic ⟩hwankyoung.ko@leeko.com⟨/13:italic⟩); **Sunghee Chae** *(Partner), Lee & Ko* (⟨13:italic ⟩sunghee.chae@leeko.com⟨/13:italic⟩); *and* **Kyung Min Son** *(Partner), Lee & Ko* (⟨13:italic ⟩kyungmin.son@leeko.com⟨/13:italic⟩).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.