MAYER | BROWN

IP & TMT QUARTERLY REVIEW

Second Quarter 2024

HONG KONG INTERNATIONAL ARBITRATION CENTRE IMPLEMENTS ITS 2024 ARBITRATION RULES

BY
AMITA HAYLOCK, PARTNER
MAYER BROWN, HONG KONG AND SINGAPORE

JENNIFER HUANG, ASSOCIATE
MAYER BROWN, NEW YORK

MALEEHA KHAN, ASSOCIATE
MAYER BROWN, NEW YORK

Complex international disputes are increasingly resolved through international arbitration, and IP & TMT disputes are no exception to this rising trend.[1] Although IP & TMT disputes were historically settled before national courts, more and more companies are drawn to the advantages of arbitration over litigation, which include a tailored, one-stop multijurisdictional resolution to the dispute, confidentiality, the ability to appoint subject-matter specialists as arbitrators, and ease of enforcement in 172 countries under the New York Convention.

Another advantage of international arbitration over litigation is that the procedural rules of major arbitral institutions are regularly updated, based on input from users of the rules (parties, arbitrators, and counsel) in the real world.

Asia dominates the top three slots for the most popular seats in international arbitration, with Singapore and Hong Kong coming in second and third, respectively, behind only London.[2] The Hong Kong International Arbitration Centre ("**HKIAC**" or "**Centre**") is one of the

1 90% of respondents in a survey preferred international arbitration for resolving cross-border disputes. https://arbitration.qmul.ac.uk/media/arbitration/docs/LON0320037-QMUL-International-Arbitration-Survey-2021_19_WEB.pdf.

2 https://arbitration.qmul.ac.uk/media/arbitration/docs/LON0320037-QMUL-International-Arbitration-Survey-2021_19_WEB.pdf.

most popular international arbitration centres in the world, reporting a record high of disputes referred to it in 2023. HKIAC-administered arbitration can be particularly interesting to IP rights holders, as the HKIAC has a panel of arbitrators specifically dedicated to IP disputes.

On 1 June 2024, the new 2024 HKIAC Rules ("**2024 Rules**") came into effect. These Rules reflect the dynamic landscape of international arbitration and contain guidance to address issues that have plagued the practice in recent years. These amendments are designed to promote the efficiency of international arbitration as a popular dispute resolution mechanism. They are the first such update since the 2018 HKIAC Rules ("**2018 Rules**"), as discussed earlier in May.

KEY CHANGES – 2018 RULES VS. 2024 RULES

WRITTEN COMMUNICATIONS

Article 3.1(f) of the 2024 Rules is a new addition. This provision specifically allows for written communications deemed to be received by a party, arbitrator, emergency arbitrator, or the HKIAC if communicated through "any other form of electronic communication that the parties have agreed to use, subject to approval by HKIAC and the arbitral tribunal, once constituted." This addition specifically acknowledges the changing technological landscape in which arbitrations are conducted, including the prevalence of the use of instant-messaging platforms.

However, some instant-messaging and other electronic communications platforms may raise questions about privacy and data security. This needs to be considered, taking into account that one of the most attractive features of arbitration to commercial parties looking to resolve their disputes outside the lens of public scrutiny. As addressed in more detail below, this concern is somewhat mitigated by the also newly-added information security provision in Article 45A of the 2024 Rules. A number of platforms that have already implemented end-to-end encryption of messages. Notably, the HKIAC has not issued further guidance with regard to specific electronic platforms, including those with end-to-end encryption. Given that this means of communications must be approved by both the HKIAC and the tribunal (after agreement by the parties), it is likely that further guidance from the Centre will be forthcoming, as it addresses these issues head-on following the implementation of the 2024 Rules.

DIVERSITY IN ARBITRATOR APPOINTMENTS

Article 9A is a new Rule requiring the HKIAC and encouraging parties and co-arbitrators to consider diversity in arbitrator appointments. This new article memorialises the HKIAC's demonstrated commitment to increase diversity in appointments.

Since 2016, when it pledged to improve equal representation in arbitration,[3] the HKIAC has seen a steady rise in the number of diverse arbitrator appointments. In 2023, the HKIAC appointed a record number of female arbitrators. The 60 female arbitrators appointed by the HKIAC constituted nearly 35% of the total 172 appointments made in 2023.[4] This increase is significantly higher than those for 2021 and 2022, which saw diverse arbitrators making up 21.8% and 27% of appointments made by the HKIAC, respectively.

INFORMATION SECURITY

Recognising the information security issues that can arise from the shifting ground of new technology, the 2024 Rules also include a new provision on information security. Similar to Article 3.1(f) which allows parties to agree to use additional means of electronic communication, Article 45A of the new Rules allows the parties to agree on reasonable measures to protect the sharing, storage, and processing of information in relation to the arbitration.

Articles 45A.2 and 13.1 specifically empower the tribunal to direct the parties and adopt suitable procedures for the conduct of the proceedings to protect the sharing, storage, and processing of information in relation to the arbitration. Article 45A.3

3 https://www.arbitrationpledge.com/organisations.

4 https://www.hkiac.org/news/hkiac-releases-statistics-2023.

goes even further, allowing the tribunal, after consultation with the parties, to make a decision, order, or award in respect of breaches of measures related to information security, as agreed by the parties or directed by the tribunal. The sensitive nature of information security, the need to protect its dissemination, and the increasing number of information-sharing platforms available may pose unique challenges for arbitrators and parties.

ENVIRONMENTAL IMPACT

Article 13.1 of the 2024 Rules expressly provides that the tribunal should also consider the environmental impact of any procedures adopted. Article 34.4(f) now also expressly includes the tribunal's consideration of "any adverse environmental impact arising out of the parties' conduct in the arbitration" in its costs award. This, again, reflects the Centre's commitment to pledges made, such as the Campaign for Greener Arbitrations, a global initiative to raise awareness of the carbon footprint of international arbitration.[5]

Even before the implementation of the 2024 Rules, many tribunals around the world had incorporated directions to move to "greener arbitrations." For example, some tribunals began moving to electronic-only submissions by the parties, eliminating the need to print thousands of pages of documents for the arbitrators and opposing counsel, who often read the electronic versions of the same documents. Relatedly, the continuation of virtual proceedings following the COVID-19 pandemic can further reduce the environmental impact of international arbitration. Although virtual proceedings may not be desired by all parties or arbitrators, in 2023 alone, 44 of the 101 hearings hosted by the HKIAC were fully or partially virtual. Given that 89.7% of HKIAC-administered arbitrations are international in nature, parties may choose to conduct their arbitrations virtually, for environmental, cost, or convenience reasons.

EXPRESS CASE MANAGEMENT AUTHORITY

Article 13.6 is another new provision geared towards efficient conduct of the case. After consultation with the parties, this provision allows the tribunal to determine preliminary issues it considers "could dispose of all or part of the case, bifurcate the proceedings, conduct the arbitration in sequential stages, and decide the stage of the arbitration at which any issue or issues shall be determined."

Bifurcation of proceedings or conducting proceedings in sequential stages promotes time- and cost-efficiency by allowing a decision on discrete issues such as jurisdictional objections prior to full briefing on the merits and quantum of the dispute, especially as that determination could ultimately result in the dismissal of a claimant's claims. While the tribunal's authority to conduct the proceedings in an efficient manner has long been broadly interpreted to include the authority to bifurcate proceedings, this new provision confirms and memorialises this widely-accepted practice.

AVOIDING CONFLICTS OF INTEREST

The 2024 Rules also include a new provision on conflicts of interest. Specifically, the tribunal may, after consulting with the parties, take necessary measures to avoid conflicts of interest arising from a change in party representation (counsel). These measures could take the form of excluding the proposed new party representative from participating in the arbitration. This provision, while new for the HKIAC Rules, is not new for peer arbitral institutions. For example, provisions expressly affording the tribunal the authority to exclude a change in party representation appear in both the 2020 London Court of International Arbitration ("**LCIA**") Arbitration Rules[6] and the 2021 International Chamber of Commerce's ("**ICC**") Arbitration Rules.[7] By contrast, such authority is absent from the 2016 Singapore International Arbitration Centre ("**SIAC**") Arbitration Rules.

5 https://www.hkiac.org/news/hkiac-releases-statistics-2023.

6 2020 LCIA Arbitration Rules, Article 18.4.

7 2021 ICC Arbitration Rules, Article 17.

PRESERVING EFFICIENCY AND INTEGRITY

Article 13.10 of the 2024 Rules specifically empowers the HKIAC, after consulting with the parties and the tribunal, to take measures necessary to preserve the efficiency or integrity of the arbitration. This includes, in "exceptional circumstances," revoking the appointment of any arbitrator where the Centre "considers that the arbitrator is prevented from or has failed to fulfil his or her functions in accordance with the Rules or within the prescribed time limits." This language is broader than and in addition to the process to challenge the appointment of an arbitrator under Article 11 of the 2024 Rules (which remains unchanged from the 2018 Rules).

Under the 2018 Rules, the only express authority in terms of conduct of the proceedings that the HKIAC had was to suspend the arbitration. The 2018 Rules (similar to the 2016 SIAC Arbitration Rules)[8] did allow the HKIAC to revoke an arbitrator appointment, but that was limited to joinder of additional parties and consolidated proceedings.[9] Article 13 broadens the scope of the HKIAC's authority to revoke an arbitrator's appointment by including this provision in the Rules concerning the tribunal's general authority to conduct the proceedings in a way that preserves the efficiency or integrity of the arbitration. It remains to be seen what the HKIAC would consider "exceptional circumstances" in practice.

SINGLE ARBITRATION UNDER MULTIPLE CONTRACTS

Another new provision, Article 29.2, relates to designation of the tribunal in single arbitrations under multiple contracts. Article 29.2 states that where the HKIAC decides that the arbitration has properly been commenced under Article 29, the parties "shall be deemed to have waived their rights to designate an arbitrator. HKIAC shall appoint the arbitral tribunal with or without regard to any party's designation." Previously, under the 2018 Rules, the HKIAC would appoint the tribunal only where claims were consolidated or involved multiple parties. Article 29.2 of the 2024 Rules is in addition to the provisions on consolidated proceedings, which remain unchanged in Article 28.

This is quite unique. While both the 2021 ICC Arbitration Rules and the 2020 LCIA Arbitration Rules confer on their respective appointing authorities the power to appoint arbitrators in the case of consolidated proceedings or proceedings involving multiple parties, they do not deem the parties' right to appoint the tribunal waived in instances involving multiple contracts under a single arbitration.[10] The 2021 ICC Arbitration Rules contain a separate provision on multiple contracts but do not empower the ICC Court to appoint the tribunal, with or without regard to the parties' designations.[11]

The 2016 SIAC Arbitration Rules also provide for multiple contracts in one arbitration.[12] SIAC Rule 8.12 provides that where an application for consolidation is granted, any party that has not nominated an arbitrator or otherwise participated in the constitution of the tribunal shall be deemed to have waived its right. Although this is similar to the new Article 29.2 of the 2024 HKIAC Rules, it is more limited in scope, excluding only parties that have not otherwise participated in the tribunal's constitution.

CLOSE OF PROCEEDINGS AND TIME LIMIT FOR RENDERING AN AWARD

Article 31.1 of the 2024 Rules now sets a time for the close of the proceedings. Previously, the 2018 Rules only stated that when the tribunal determines that the parties have had a reasonable opportunity to present their case, it shall declare the entire proceedings closed or declare closed a relevant part of the proceedings. While the 2024 Rules maintain this language, it is qualified by noting that "no later than 45 days from the last directed substantive oral or written submissions" shall the tribunal declare the entire proceedings or

8 2016 SIAC Arbitration Rules, Rules 7.6-7.7, 8.10-8.11.
9 2018 HKIAC Arbitration Rules, Articles 27-28.
10 2021 ICC Arbitration Rules, Article 10; 2020 LCIA Arbitration Rules, Article 8.
11 2021 ICC Arbitration Rules, Article 9.
12 2016 SIAC Arbitration Rules, Rule 6.1.

relevant part of the proceedings closed. Article 31.2 of the 2024 Rules maintains that an award shall be rendered within three months of the close of the proceedings in whole or in part. Setting a specific time limit for closure of the proceedings should promote greater efficiency of tribunals' decision-making and render an award to the parties in a more timely fashion.

The SIAC Rules have a different approach on the time limit for rendering an award. While the SIAC Rules do not impose a limit on the close of the proceedings, as the new 2024 HKIAC Rules do, SIAC Rule 32.3 requires the tribunal to submit a draft award to the SIAC Registrar no later than 45 days from the date on which proceedings are declared closed. After the Registrar reverts back with its comments on the draft award, the SIAC Rules do not provide a timeline for the tribunal to render the final award.

ARBITRATION COSTS

Article 34.1(f) of the 2024 Rules now expressly allows the tribunal's costs award to include the costs of any Emergency Relief proceedings. Article 34.4 also sets forth a non-exhaustive list of factors the tribunal may consider when apportioning costs, including: "(a) the relative success of the parties; (b) the scale and complexity of the dispute; (c) the conduct of the parties in relation to the proceedings; (d) any third party funding arrangement; (e) any outcome related fee structure agreement; and/or (f) any adverse environmental impact arising out of the parties' conduct in the arbitration." Previously, under the 2018 Rules, the tribunal had general authority to apportion costs "taking into account the circumstances of the case," including any third-party funding arrangement. Thus, the 2024 Rules still allow tribunals to take into account the circumstances of the case, while providing an illustrative list of factors for consideration.

A particularly noteworthy addition to Article 34.4 is the tribunal's consideration of "any outcome related fee structure agreement" in its costs determination. Some third-party funding agreements specifically exclude the funder's responsibility to pay for an adverse costs award. This means that if a party (typically a claimant) is not successful in its claim and is ordered to pay the other party's legal fees and costs in the arbitration, the third-party funder is not liable to pay for those fees and costs. This can create problems, particularly where a party is in need for third-party funding in the first place often because of its financial inability to pursue the arbitration on its own. To further complicate matters, tribunals may not have jurisdiction over the third-party funder to enforce a costs award because the funder is not a signatory to the underlying arbitration agreement or a party to the arbitration proceedings.

Historically, arbitral institutions have dealt with the disclosure of third-party funding in the broader context of arbitrator independence and impartiality. This is true of both the LCIA and SIAC Rules. The LCIA Rules on arbitrator impartiality and independence state that the arbitrators shall remain impartial and independent of the parties and that they have a continuing obligation to disclose material information that would create justifiable doubts as to their independence and impartiality throughout the proceeding.[13]

This Article is similar to others, including the HKIAC and SIAC Rules. However, the SIAC Rules provide for the disclosure of third-party funders given the likelihood of third-party funders to potentially impact the independence and impartiality of the tribunal. Although not specifically in the 2016 SIAC Rules, in March 2017, SIAC issued a practice note noting that the tribunal shall have the power to conduct inquiries that appear to be necessary or expedient, including "ordering the disclosure of the existence of any funding relationship with an External Funder and/or the identity of the External Funder and, where appropriate, details of the External Funder's interest in the outcome of the proceedings, and/or whether or not the External Funder has committed to undertake adverse costs liability."[14] This Practice Note supplements an arbitrator's obligations under the SIAC Rules, meaning where applicable, the Practice Note shall have the same force and effect as the SIAC Rules themselves.

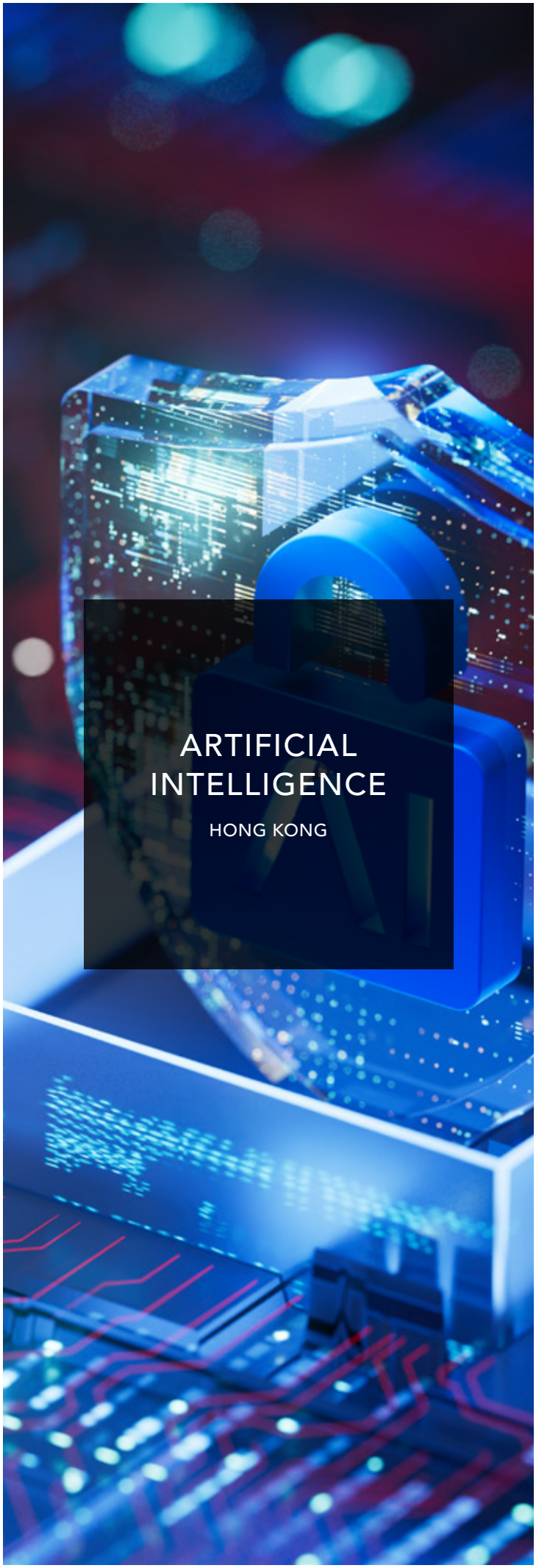
13 2020 LCIA Arbitration Rules, Article 5.

14 SIAC Practice Note dated 31 March 2017 on Arbitrator Conduct in Cases Involving External Funding. Practice-Note-for-Administered-Cases-–-On-Arbitrator-Conduct-in-Cases-Involving-External-Funding.pdf (siac.org.sg).

CONCLUSION

Overall, the 2024 Rules are designed to promote efficiency and diversity in international arbitration. Considering the competition among arbitral institutions to administer international arbitration proceedings, other institutions may soon issue their own rules updates, in light of the implementation of the 2024 HKIAC Rules. While some amendments, such as Article 13.6 (granting tribunals the express authority to bifurcate proceedings), serve to memorialise existing widely-accepted practices, the practical impact of other revisions remains to be seen, such as those involving data privacy concerns and party autonomy in arbitrator appointments.

THE AUTHORS WOULD LIKE TO THANK NITIN NAINANI, ASSOCIATE AT MAYER BROWN, FOR HIS ASSISTANCE WITH THIS LEGAL UPDATE.



THE HONG KONG PCPD ISSUES MODEL PERSONAL DATA PROTECTION AI FRAMEWORK

BY
GABRIELA KENNEDY, PARTNER
MAYER BROWN, HONG KONG

JOSHUA WOO, REGISTERED FOREIGN LAWYER (SINGAPORE), MAYER BROWN, HONG KONG

INTRODUCTION

The rapid development of Artificial intelligence ("**AI**") has been the cause for much excitement over the past 2 years. Ever since the public launch of Open AI's ChatGPT on 30 November 2022, generative AI and its capabilities have been at the forefront of the public consciousness, with AI making the headlines on a daily basis.

However, the advancement and increased adoption of AI have also brought about unprecedented challenges both to businesses and regulators alike, especially in relation to personal data. Quite a few regulators in the region have issued guidance on AI[15] and, on 11 June 2024, the Hong Kong Office of the Privacy Commissioner for Personal Data ("**PCPD**") joined them by issuing the "Artificial Intelligence: Model Personal Data Protection Framework" ("**Model Framework**").[16] The release of the Model Framework follows the PCPD's previous Guidance Note titled "Guidance on the Ethical Development and Use of Artificial Intelligence" ("**Ethical AI Guidance Note**") issued in August 2021;[17] and the Office of the Government Chief

15 See the Singapore Personal Data Protection Commission's Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems issued on 1 March 2024; the Indonesian Ministry of Communication and Informatics Circular Letter on AI Ethical Guidelines issued on 19 December 2023; the Japanese Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry AI Operator Guidelines issued on 19 April 2024.

16 Available here: https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_protection_framework.pdf.

17 Available here: https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf.

Information Officer's "Ethical Artificial Intelligence Framework", first released in September 2022 and last updated in August 2023.[18]

While the 2021 Ethical AI Guidance Note was primarily aimed at organisations that *develop* AI systems, the Model Framework now targets all organisations that procure, implement, and use AI systems involving personal data.

The Model Framework adopts a risk-based approach,[19] and aligns with PCPD's previous recommendations in the Ethical AI Guidance Note to provide practical recommendations to organisations looking to adopt AI solutions, while remaining compliant with the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**").[20]

The Model Framework is based on three data stewardship values and seven ethical principles that were first articulated in the 2021 Ethical AI Guidance Note, namely:

DATA STEWARDSHIP VALUES

1. Being Respectful
2. Being Beneficial
3. Being Fair

and

ETHICAL PRINCIPLES FOR AI

1. Accountability
2. Human Oversight
3. Transparency and Interpretability
4. Data Privacy
5. Beneficial AI
6. Reliability, Robustness and Security
7. Fairness

THE MODEL FRAMEWORK

The Model Framework consists of four parts:

1. AI Strategy and Governance;[21]
2. Risk Assessment and Human Oversight;[22]
3. Customisation of AI Models and Implementation and Management of AI Systems;[23] and
4. Communication and Engagement with Stakeholders,[24]

though this framework was actually broadly set out in the Ethical AI Guidance Note in 2021. The 2024 Model Framework replaces "Development of AI Models and Management of AI Systems" with the "Customisation of AI Models and Implementation and Management of AI Systems", likely in recognition of commercial realities (i.e. various new applications built on a few pre-existing, established AI models), and also goes a step further by providing specific practical recommendations and examples that will help organisations to get a better sense of what steps to take when procuring, implementing and using AI systems that are heavily reliant on personal data.

This article provides a high-level summary of the Model Framework.

1. AI STRATEGY AND GOVERNANCE

The Model Framework emphasises the importance of top management buy-in and participation in deploying ethical AI,[25] and recommends that organisations should establish an internal AI governance strategy that comprises of (a) an **AI strategy**; (b) **governance considerations** for AI procurement; and (c) an **AI governance steering committee**.

18 Available here: https://www.ogcio.gov.hk/en/our_work/infrastructure/methodology/ethical_ai_framework/doc/Ethical_AI_Framework.pdf.
19 Model Framework, paragraph 12; see also Ethical AI Guidance Note, page 12.
20 Model Framework, paragraph 8.
21 Model Framework, part 1.
22 Model Framework, part 2.
23 Model Framework, part 3.
24 Model Framework, part 4.
25 Model Framework, paragraph 13.

The AI strategy should:[26]

i. define the role of the deployed AI systems within the organisation's greater technological ecosystem;
ii. set out the organisation's guiding ethical principles in regards to AI;
iii. delineate what scenarios the organisation deems as unacceptable use of AI;
iv. establish an AI inventory;
v. set out specific internal policies and procedures for the ethical procurement, implementation and use of AI solutions;
vi. establish technical infrastructure for lawful, responsible, and quality AI use;
vii. require regular sharing of the AI strategy with all relevant personnel and, where relevant, external stakeholders;
viii. consider applicable and upcoming laws relevant to AI procurement, implementation, and use; and
ix. require continual refining based on feedback from the Model Framework's implementation.

The Model Framework also suggests governance considerations for procuring AI solutions, such as understanding the purposes of AI use, privacy and security obligations, international standards, criteria for evaluating AI solutions and suppliers, potential risks arising from use, relevant contractual protections (e.g. data processing agreements), policy on the use of outputs, and a feedback mechanism for monitoring the solution.[27]

The Model Framework recommends establishing an AI governance steering committee to ensure accountability and human oversight. Notably, this governance committee should entail participation from senior management and members across various departments, including a C-level executive to lead the committee. The committee would report to the board and oversee the entire life cycle of all AI solutions, and be responsible for designating clear roles for the various internal stakeholders in the life cycle of the AI system, ensuring adequate resourcing, establishing effective monitoring mechanisms, and providing training to raise awareness for all relevant personnel.[28]

2. RISK ASSESSMENT AND HUMAN OVERSIGHT

Following an organisation's establishment of its AI Strategy and Governance, the next part of the Model Framework involves the identification and evaluation of risks posed by AI systems and the adoption of corresponding mitigation measures.[29]

The Model Framework sets out a number of non-exhaustive risk factors that organisations should consider, including the allowable uses of data, the volume and sensitivity of data used, data quality, the security of personal data and the probability of privacy risks arising weighed against the potential severity of harm.[30]

It also provides that the level of human oversight should correspond to the risk level of the AI system (i.e., the potential impact the output might have on individuals), ranging from "human-in-the-loop" to "human-out-of-the-loop" approaches.[31] Furthermore, the Model Framework acknowledges the potential trade-offs that may need to be addressed, such as balancing predictive accuracy against explainability of AI output; data minimisation against statistical accuracy,[32] and recommends the documentation of an organisation's assessment and the rationale underlying its decisions.

3. CUSTOMISATION OF AI MODELS AND IMPLEMENTATION AND MANAGEMENT OF AI SYSTEMS

Part 3 of the Model Framework addresses the "execution" phase to prepare the AI solution for the

26 Model Framework, paragraph 14.
27 Model Framework, paragraph 16.
28 Model Framework, paragraphs 20 to 23.
29 Model Framework, paragraph 24.
30 Model Framework, paragraph 27.
31 Model Framework, paragraph 32.
32 Model Framework, Part 2.3; see also Figure 13.

organisation's specific purposes. This is envisioned to involve preparation of data to train the AI model to understand the organisation's context-specific requirements, the fine-tuning of the AI model with this data, and the management and monitoring of the AI solution's performance.

DATA PREPARATION

In order to ensure compliance with the PDPO, two key focus areas are recommended for the preparatory phase namely data minimisation, to ensure that individuals' personal data privacy is protected and data quality, to ensure that the resulting output is fair and unbiased.[33]

FINE-TUNING / CUSTOMISATION AND IMPLEMENTATION

Following the application of the prepared data to the AI solution, the Model Framework advocates rigorous testing to validate the AI solution and ensure fairness in a manner that is proportionate to the potential risks.[34] In particular, organisations should take the following steps when implementing AI solutions:

i. confirm that the AI solution meets procurement requirements;
ii. conduct AI solution tests;
iii. perform User Acceptance Tests;
iv. implement transparency, traceability, and auditability mechanisms;
v. establish security measures against adversarial attacks; and
vi. address the legal and security aspects of AI system hosting.

MANAGEMENT AND MONITORING

Additionally, the Model Framework stresses the need for continuous management and monitoring of AI systems, including the documentation of responses to anomalies in the datasets, risk reassessments (relating to the inputs, outputs and AI supplier), periodic reviews of the AI model to ensure it is functioning as intended, human oversight, continuous feedback from users, an evaluation of the AI landscape as a whole, the establishing of an AI Incident Response Plan and periodic internal AI audits. [35]

4. COMMUNICATION AND ENGAGEMENT WITH STAKEHOLDERS

The final part of the Model Framework highlights the role of transparency in AI systems for building trust with stakeholders.[36] It highlights the importance of the provision of information (i.e. in the organisation's Personal Information Collection Statement and Privacy Policies), mechanisms for data access, data correction and feedback as key elements of communication and engagement.[37]

Where organisations may use personal data to customise and train AI solutions, they should consider informing data subjects:

i. that their personal data will be used for AI training and / or customisation, or facilitating automated decision-making and so on;
ii. of the classes of persons to whom the data may be transferred, e.g., the AI supplier;
iii. of the organisation's policies and practices in relation to personal data in the context of customisation and use of AI.

Organisations are strongly encouraged to practice "Explainable AI", ensuring that the decisions and output of AI systems are explainable to stakeholders.[38] Where AI systems have the potential to significantly impact individuals, the explanations should include:[39]

i. the AI system's role in the decision-making process, including key tasks for which it is responsible and any human involvement;

33 Model Framework, paragraph 41; see also Figure 15 and Example 2 on Page 36.
34 Model Framework, paragraph 43; see also Figure 16.
35 Model Framework, paragraphs 47 - 50.
36 Model Framework, paragraph 51.
37 Model Framework, paragraphs 55 to 57.
38 Model Framework, paragraph 58.
39 Ibid.

ii. the relevance and necessity of the personal data in the AI-assisted processes; and

iii. the major factors in the AI system's overall and individual decisions. If such explanations are not feasible, the organisation should explicitly explain why.

The Model Framework further recommends the disclosure of AI system use, along with the associated risks and results of conducted risk assessments; as well as providing options for explanation, human intervention, and data subjects to opt-out.[40] It also encourages providing explanations for AI decisions and output, where feasible, and using plain language and accessible formats for communication.[41]

CONCLUSION

The Model Framework builds on the 2021 Ethical AI Guidance Note and serves as a checklist for companies adopting AI tools in their business operations. The recommendations and risk assessments required offer a road map for companies. While unlike the EU AI act the Model Framework is not law, it signals the expectations of the privacy regulator and the line of enquiries that will be pursued in the event of a data breach stemming from the use of AI tools. What this means for companies is that the assessment of risks when adopting AI tools have to be documented as articulated in the Model Framework. This includes receiving written assurances from third party suppliers that their AI systems measure up to the yardsticks in the Model Framework. The responsibility for this remains with AI steering committees that organisations will need to set up.

Organisations that procure, implement, and use AI systems involving personal data should therefore refer to the Model Framework and follow the recommendations within to build trust with stakeholders and ensure compliance with the PDPO. when deploying AI solutions. We expect that the PCPD will continue to monitor and update the Framework as AI technologies and regulations evolve; as well as continue to engage with various stakeholders and sectors to promote the ethical and responsible use of AI in Hong Kong.

THE AUTHORS WOULD LIKE TO THANK CALVIN TAN, TRAINEE SOLICITOR AT MAYER BROWN, FOR HIS ASSISTANCE WITH THIS LEGAL UPDATE.

40 Model Framework, Figure 20.

41 Model Framework, paragraphs 59 and 60.

BEIJING INTERNET COURT ISSUES FIRST DECISION ON PERSONALITY RIGHTS IN AI-GENERATED VOICE

BY
AMITA HAYLOCK, PARTNER
MAYER BROWN, HONG KONG AND SINGAPORE

GRACE WONG, ASSOCIATE
MAYER BROWN, HONG KONG

With an increase in the number of lawsuits brought by copyright owners against artificial intelligence ("**AI**") companies, the AI industry is under scrutiny on how it balances the protection of intellectual property rights against the rapid developments in technological advancements in AI.

Recently, Scarlett Johansson's complaint that OpenAI's voice assistant sounded very much like her has made the world's headlines, causing OpenAI to pull the use of the voice.[42] Against this background, in this article, we consider a decision issued by the Beijing Internet Court on 23 April 2024 concerning the unauthorised use of voice recordings to train an AI text-to-speech application ("**Application**").[43]

BACKGROUND

The Plaintiff is a dubbing artist who learnt that the Application was generating audio outputs in a voice that very much sounded like the Plaintiff's voice. It transpired that the Application was trained on sound recordings featuring the Plaintiff. The parties involved in the dispute and their roles are set out below:-

42 Scarlett Johansson told OpenAI not to use her voice — and she's not happy they might have anyway - The Verge

43 全國首例AI生成聲音人格權侵權案一審宣判 (qq.com)

PLAINTIFF	Dubbing artist.
1ST DEFENDANT	Beijing technology company which incorporated the Application into its online platform.
2ND DEFENDANT	Beijing culture and media company which commissioned the Plaintiff to record sound recordings ("**Recordings**"). The 2nd Defendant owns the copyright to the Recordings and provided these to the 3rd Defendant.
3RD DEFENDANT	Software company which the 2nd Defendant permitted to use, reproduce, and modify the data of the Recordings for commercial and non-commercial purposes for the 3rd Defendant's goods and services. The 3rd Defendant used the Recordings as AI training material and developed the Application.
4TH DEFENDANT	A Shanghai network technology company. The 3rd Defendant put the Application onto the 4th Defendant's cloud service platform for sale.
5TH DEFENDANT	Beijing technology development company which entered into an online service sales contract with the 1st Defendant and placed an order with the 3rd Defendant for the 1st Defendant's use of the Application.

INFRINGEMENT OF PERSONALITY RIGHTS

Unlike jurisdictions such as Hong Kong and the United Kingdom, personality rights are a statutory right under the Civil Code of the People's Republic of China ("**PRC**"). An individual has the right to use or publish his/her likeness or permit another person to do so; without such consent, no one can use exploit, defame, or forge an individual's likeness.[44] Such protection is expressly extended to an individual's voice.[45]

The Court in this case further recognised this by noting the voice of an individual is unique and distinctive due to different voice patterns, timbres, and frequencies. A voice is deemed to be identifiable if it can be associated with a specific individual through repeated or prolonged listening. Even if the voice is synthesised by AI, it can be identifiable if the general public or the public in the relevant field is able to associate it to an individual.

Upon the Court's investigation, it agreed with the Plaintiff that the voice generated by the Application had a high degree of similarity with the Plaintiff's voice in terms of the timbre, tone, and vocal style. As an ordinary listener would be able to associate the AI voice with the Plaintiff, the Plaintiff's personality rights covered the AI voice in question.

LIABILITY

Whilst the 2nd Defendant owned the copyright of the Recordings, the Court clarified this did not entitle the 2nd Defendant to authorise the use of the Recordings for AI training purposes without the Plaintiff's consent. The fact that the 2nd and 3rd Defendants entered into a contract for the use of the Recordings for this purpose does not confer a legal basis for such unauthorised use. Therefore, the 2nd and 3rd Defendants had infringed the Plaintiff's personality rights.

As for the remaining defendants, the Court did not consider them to be subjectively at fault – therefore ruling that they are not liable for damages to the Plaintiff.

The 1st and 3rd Defendants were ordered to apologise to the Plaintiff, whereas the 2nd and 3rd Defendants were ordered to pay compensation of RMB 250,000 to the Plaintiff.

44 Articles 1018 to 1020, Civil Code of the PRC
45 Article 1023, Civil Code of the PRC

POSITION IN HONG KONG

As mentioned above, personality rights are not recognised in Hong Kong by statute or common law. There is no free-standing right under Hong Kong law to control the use of one's name, image, or voice. Nevertheless, a creator like the Plaintiff could rely on the common law tort of passing off. This would require the claimant to establish the "classical trinity" of the claimant's goodwill; the respondent's misrepresentation; and damage or the likelihood of damage to the claimant by the misrepresentation.

Whilst there has yet to be a successful case of endorsement as passing off in Hong Kong, the Hong Kong Court of First Instance has previously noted there is no "*general proposition that the mere use of an artist's or composer's name, image or likeness on the subject products can never amount to any misrepresentations relating to those products, so as to constitute a cause of action based on passing off.*"[46] There is also a long line of English cases confirming the cause of action covers a misrepresentation that the claimant has endorsed the goods or services of the respondent.[47] Specifically, in as early as 1958, the UK High Court recognised that "*it would seem [to be] a grave defect in the law if it were possible for a party, for the purpose of commercial gain, to make use of the voice of another party without his consent.*"[48]

CONCLUSION

In the Asia Pacific region, the PRC is known to be proactive in AI governance and regulation, for example with provisions and measures on algorithmic recommendations and generative AI services. It is encouraging to see that in addition to such regulations, the PRC courts have tried to balance creators' rights and endeavours with innovation and technological advancement. Whilst copyright and trademark issues are taking centre stage in legal battles over AI, this recent decision helpfully shows us that personality rights and passing off offer creators options in protecting their rights in the burgeoning AI landscape.

THE AUTHORS WOULD LIKE TO THANK ROSLIE LIU, INTELLECTUAL PROPERTY OFFICER AT MAYER BROWN, FOR HER ASSISTANCE WITH THIS LEGAL UPDATE.

46 Liu Chia Chang v. Worldstar Music International Ltd (13/02/2007, HCA1470/2006) para. 28

47 For example: *Fenty v Arcadia Group Brands Ltd* [2015] EWCA Civ 3; *Irvine & Ors v TalkSport Ltd* [2003] EWCA Civ 423

48 Judgment of McNair J. in *Sim v HJ Heinz Co Ltd* [1958] 12 WLUK 81; full text reproduced in *Sim v H. J. Heinz Co. Ltd. and Another* [1959] 1 W.L.R. 313

CHINA EASES CONTROLS OVER CROSS-BORDER DATA TRANSFERS

BY
GABRIELA KENNEDY, PARTNER
MAYER BROWN, HONG KONG

JOSHUA WOO, REGISTERED FOREIGN LAWYER (SINGAPORE), MAYER BROWN, HONG KONG

On 22 March 2024, the Cyberspace Administration of China ("**CAC**") issued the hotly-anticipated Provisions on Promoting and Regulating Cross-Border Data Transfers (the "**CBDT Provisions**").[49] This comes nearly six months after the CAC announced a relaxation of some of the onerous cross-border data transfer requirements in September 2023 (the "**Draft**") (see our previous Legal Update on China Proposes easing of Cross-border Data Controls). The CBDT Provisions introduce welcome exemptions from certain categories of exports, while also clarifying pre-existing ambiguities in the cross-border data transfer regime.

The CAC also concurrently released the Guidelines for the Filing of Standard Contracts for Exporting Personal Information (Second Version) ("**SC Guidelines V2**") and the Guidelines for the Application of Security Assessment for Exporting Personal Information (Second Version) ("**Security Assessment Measures V2**") (collectively, the "**New Guidelines**"),[50] which echo the revised requirements set out in the CBDT Provisions and provide revamped processes for complying with the various cross-border data transfer mechanisms that companies are required to implement.

Both the CBDT Provisions and New Guidelines came into force with immediate effect, though the CBDT Provisions take precedence in the event of any conflict

49 Original texts can be found here: https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm

50 Original texts can be found here: https://www.cac.gov.cn/2024-03/22/c_1712783131692707.htm

with the first versions of the SC Guidelines and Security Assessment Measures.[51]

In this article, we look at the key changes in the finalised CBDT Provisions and the New Guidelines and highlight relevant considerations that data controllers should look out for.

EXEMPTIONS FROM CROSS-BORDER DATA TRANSFER MECHANISMS

Under the CBDT Provisions, the following cross-border data transfers are exempted from the requirements set out in Article 38 of the Personal Information Protection Law ("**PIPL**") (i.e., the Security Assessment, Certification, and Standard Contract (together, the "**Cross-Border Data Transfer Mechanisms**"):

1. Cross-border transfers of data generated from activities such as:
   a. international trade;
   b. cross-border transport;
   c. academic cooperation;
   d. cross-border manufacturing; or
   e. marketing

   that **do not** contain personal information or important data;[52]
2. Personal information that is collected or generated out of the PRC and subsequently processed within the PRC, provided that there is no introduction of any personal information or important data during the processing (i.e. data handled by PRC-based data processors who may export personal information that was previously imported);[53]
3. Data which is necessary for the performance of a contract to which the data subject is a party, such as for the purposes of:
   a. cross-border e-commerce;
   b. cross-border shipping;
   c. cross-border remittance;
   d. cross-border payments;
   e. cross-border account opening;
   f. plane ticket and hotel bookings;
   g. examination service; and
   h. visa applications;[54]
4. Employee data that is necessary for human resources (HR) management in accordance with legally formulated labour policies or collective employment contracts;[55]
5. Cross-border data transfers that are necessary for protecting the health and safety of a natural person in an emergency;[56]
6. Data transferred by data controllers (who are not critical information infrastructure operators) provided that such transfers cumulatively do not exceed the data of 100,000 individuals and such data does not include sensitive data, since 1 January of the current year;[57] and
7. Cross-border data transfers falling outside the negative list to be formulated by Free Trade Zones (FTZs).[58]

BROADENED EXEMPTIONS

When compared to the Draft, categories (1) and (3) above have been broadened in the CBDT Provisions to include more scenarios such as cross-border transport, cross-border shipping, cross-border payment,

51 Article 13 of the CBDT Provisions specifically provides that the CBDT Provisions shall prevail over any conflicts with the Measures for Security Assessment for Cross-Border Data Transfers ("**Security Assessment Measures**") and the Measures on Standard Contracts for the Export of Personal Information ("**SC Measures**").

52 Article 3 of the CBDT Provisions

53 Article 4 of the CBDT Provisions

54 Article 5(1)) of the CBDT Provisions

55 Article 5(2)) of the CBDT Provisions

56 Article 5(3)) of the CBDT Provisions

57 Article 5(4)) of the CBDT Provisions

58 Article 6 of the CBDT Provisions

cross-border account opening and examination services. Arguably, the first category is unnecessary as it clearly refers to data that does not fall within the ambit of PIPL.

The threshold in (6) above has also been significantly raised from 10,000 to 100,000 individuals. Notably, unlike the Draft,[59] the CBDT Provisions now specify that the relevant date for determining when a data controller falls within the threshold is 1 January of the ***current*** year, instead of the ambiguously worded "*within one year*" used in the Draft that potentially signalled a constantly changing yardstick.

The broadened exemptions have a significant positive effect on companies engaged in activities identified in (1) and (3) above, which, prior to the CBDT Provisions, would have had to utilise one of the Cross-Border Data Transfer Mechanisms. The increased threshold set out in (6) above also substantially eases the compliance burden of small and medium-sized data controllers in the PRC that are engaged in cross-border data transfers involving less than 100,000 individuals.

The CBDT Provisions also clarify the scope of the exemption applicable to personal information collected outside of the PRC. The wording of this exemption in the Draft[60] engendered some confusion given that the cross-border data transfer rules did not ostensibly apply to personal information collected outside the PRC, though this has now been clarified in (2) above to exempt personal information initially collected out of the PRC and subsequently processed within the PRC (as long as there is no introduction of any personal information or important data during the processing).

This is a welcome clarification for overseas data controllers who may process personal information in the PRC, as well as for PRC-based data processors, who do not need to utilise any of the Cross-Border Data Transfer Mechanisms in respect of "imported" personal information.

NEW THRESHOLDS FOR CROSS-BORDER DATA TRANSFER REGIME

Under the CBDT Provisions, data controllers will be subject to the security assessment if they have cumulatively exported:[61]

1. the personal information (excluding sensitive personal information) of **1 million people**; or
2. the sensitive personal information of 10,000 people

since 1 January of the current year. Meanwhile, data controllers that have cumulatively exported the personal information of more than 100,000 people but fewer than 1 million people, or the sensitive personal information of fewer than 10,000 people since 1 January of the current year are required to carry out the Certification or to utilise the Standard Contract ("**SC**").[62]

The CBDT Provisions remove the volume of personal information processed as a trigger for the Security Assessment,[63] and focus the inquiry on the volume of personal information cumulatively exported instead. In addition, the data export threshold that triggers the Security Assessment has been raised from 100,000 people since 1 January of the previous year to 1 million people since 1 January of the current year, though exports of personal information by Critical Information Infrastructure Operators ("**CIIOs**") and exports of important data are still subject to the Security Assessment.[64]

Nevertheless, the proposed provision regarding the transfer of important data in the Draft has been

59 Article 5 of the Draft CBDT Provisions provides that "*cross-border data transfers by data controllers that **expect** to transfer the personal information of less than 10,000 individuals out of the PRC **within a year** are exempted from the transfer mechanisms requirements set out in Article 38 of the PIPL.*"

60 Article 3 of the Draft CBDT Provisions provided that "Personal information that is not collected in China and provided overseas, do not need to apply for a security assessment for data export, conclude a standard contract for personal information export, or pass personal information protection certification."

61 Article 7 (2), the CBDT Provisions

62 Article 8, the CBDT Provisions

63 Under Article 4(2) of the Security Assessment Measures, data controllers who processed the personal information of over 1 million people that provided personal information abroad would be subject to the security assessment.

64 Article 7, the CBDT Provisions

retained, allowing data controllers to proceed on the presumption that they do not process "important data" unless they have been informed by the regulators or through a public notice that specified types of data in their possession has been classified as "important data".[65]

The Security Assessment has proved very difficult to achieve, with only a handful of data controllers having passed this assessment since the grace period for the Security Assessment measures expired on 1 March 2023. While the SC has not proved to be as convenient as initially expected, the relaxation of the Security Assessment thresholds will no doubt bring significantly relief to data controllers who export the personal information of fewer than 1 million individuals and who were unable to pass the Security Assessment or have simply adopted a "wait-and-see" approach.

VALIDITY OF SECURITY ASSESSMENT

The CBDT Provisions have also extended the validity of the Security Assessment from two to three years, easing the procedural burden of companies that are still subject to the Security Assessment.[66]

Data controllers who need to export data after the expiry of their first Security Assessment, may apply for an extension of the validity of the assessment 60 working days prior to the expiration of the Security Assessment, provided there are no circumstances that would trigger the requirement to carry out a new Security Assessment.[67]

While the extension is still subject to approval from the CAC, and the requirements of the extension process are presently unclear,[68] the CBDT Provisions seem to suggest that the process for the extension of a Security Assessment validity would be easier than the initial assessment process.

KEY CHANGES TO THE SECURITY ASSESSMENT AND STANDARD CONTRACT

Unlike the previous requirement for data controllers to submit documents to the local CAC office (for more detail, please see our previous Legal Update on China's Standard Contracts for Exporting Personal Information Guidelines Have Been Released! and China's Security Assessment Measures for Cross-Border Data Transfers, Effective September 2022), the CAC now accepts Security Assessment applications and SC filings nationwide via an online portal (https://sjcj.cac.gov.cn), and has relaxed some of the more burdensome formality and evidentiary requirements. For example, the New Guidelines now waive the requirement for *original copies* of some of the documents such as the Standard Contract, the signed power of attorney, the signed letter of commitment,[69] though all copies of documents still need to be submitted via the online portal.

The New Guidelines expressly provide that the online portal submission does not apply to Security Assessment applications from CIIOs,[70] which are still required to submit paper applications together with an electronic version to the relevant CAC provincial branch offices.

The New Guidelines also provide revised versions of the Personal Information Protection Impact Assessment ("**PIPIA**") and Privacy Impact Assessment ("**PIA**") templates and remove some additional assessment matters that ostensibly go beyond the provisions of the PIPL, e.g., the impact of the policies, laws, and regulations of the foreign recipient's jurisdiction, description of the data processing by the foreign

65 Article 2, the CBDT Provisions
66 Article 9, the CBDT Provisions; Article 14, the Security Assessment Measures
67 Article 9, the CBDT Provisions
68 The Security Assessment Measures V2 do not provide any details on process for the extension of validity.
69 Article 3(1), the SC Guidelines (Second Version); Article 3, the Security Assessment Guidelines (Second Version)
70 Article 2, the Security Assessment Guidelines (Second Version)

recipient.[71] This will reduce the compliance burden, make the application for the Security Assessment and SC much easier and reduce compliance costs.

Unlike the previous PIPIA, the revised SC PIPIA appears to have excluded some of the assessment areas set out in the revised Security Assessment PIA (e.g. security capability of data controllers, data security obligations and responsibilities agreed in the agreement). The CAC' appears to have taken on board previous criticisms that the SC regime was as burdensome as the Security Assessment.

The CBDT Provisions provide a welcome easing of the thresholds, and add some clarity on the scope of the exemptions and new thresholds. However, there are still outstanding questions on the practical applicability of the new rules that remain unanswered.

For example, the CBDT Provisions remain vague in some areas such as the "necessity" threshold for HR management in exemption (4). Given the different treatment of sensitive personal information under the law, it is unclear whether the sensitive personal information of employees (e.g., financial information, medical records etc.) will fall within the HR exemption.

It is presently unclear how data controllers that were in the midst of undergoing the more stringent Security Assessment, in accordance with the previously set thresholds can proceed further given that they are now allowed to utilise the Standard Contract. Can they withdraw their Security Assessment applications currently under consideration by the CAC? Can they "convert" their applications into SC applications or will they have to start *de novo*?

TAKEAWAYS

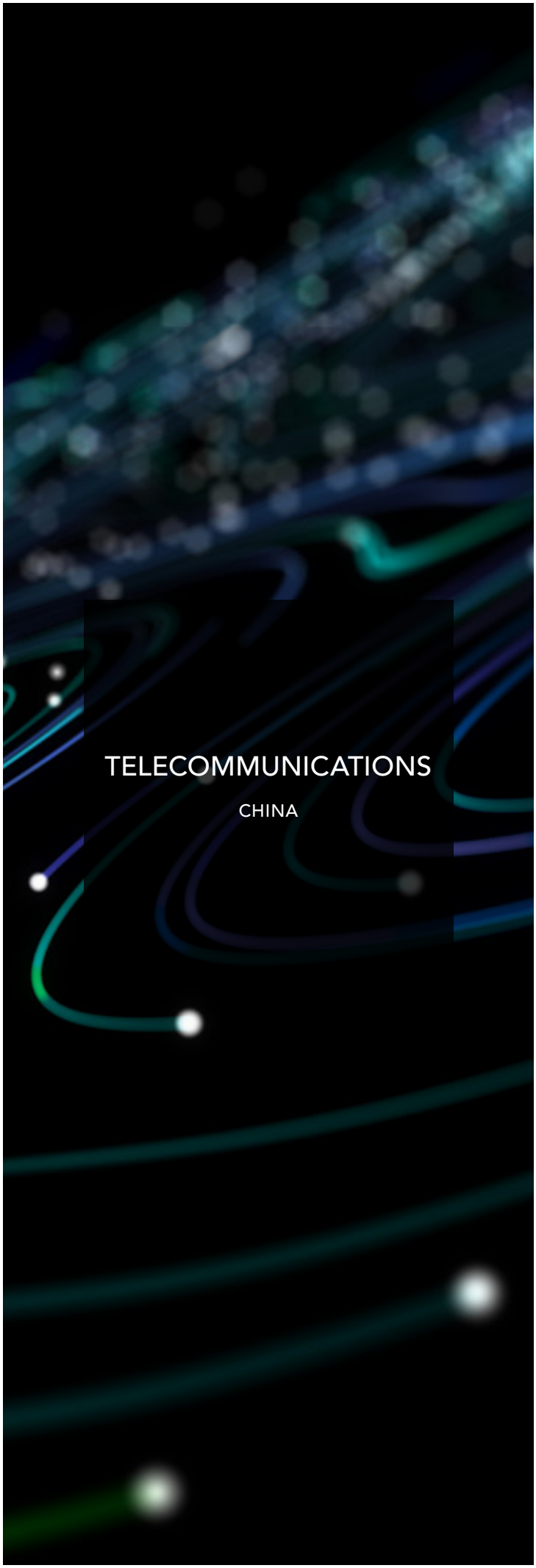
The CBDT Provision came into immediate effect and provide businesses with a greater degree of clarity as to their compliance obligations, while easing the strict thresholds promulgated by the first versions of the Security Assessment Measures and SC Guidelines. Data controllers in the PRC that engage in data exports should therefore take stock to determine if they fall within any of the new exemptions or fall below the revised thresholds provided by the CBDT Provisions and calibrate their compliance efforts accordingly.

Given the outstanding questions left unanswered by the CBDT Provisions and New Guidelines, data controllers are advised to keep an eye out for news of enforcement actions and trends, particularly in relation to employee personal information / HR data.

Additionally, given that cross-border data transfers that are not included in the negative list exempted from the Cross-Border Data Transfer Mechanisms may instead be subject to special rules to be formulated by the regulators of FTZs, data controllers with business interests in free trade zones will need to watch out for developments on the negative lists and any additional rules that may be released in the coming months.

THE AUTHORS WOULD LIKE TO THANK ROSLIE LIU, INTELLECTUAL PROPERTY OFFICER AT MAYER BROWN, FOR HER ASSISTANCE WITH THIS LEGAL UPDATE.

71 Annex 4 of the Security Assessment Guidelines (Second Version) and Annex 5 of the SC Guidelines (Second Version)



CHINA RELAXES FOREIGN INVESTMENT RESTRICTIONS ON VALUE-ADDED TELECOM SERVICES

BY
GABRIELA KENNEDY, PARTNER
MAYER BROWN, HONG KONG

JOSHUA WOO, REGISTERED FOREIGN LAWYER (SINGAPORE), MAYER BROWN, HONG KONG

On 10 April 2024, the Ministry of Industry and Information Technology of China ("**MIIT**") issued the Circular on Launching the Pilot Scheme for Expanding the Opening-up of Value-Added Telecommunications Services ("**VATS Circular**") to relax the shareholding restrictions placed on foreign investors in selected value-added telecom services ("**VATS**") in a few areas, namely the Shanghai Lin-gang and Pudong New Areas, Beijing, Shenzhen and Hainan ("**Pilot Areas**").[72]

BACKGROUND

Under the Provisions on the Administration of Foreign-Invested Telecommunications Enterprises (the "**FITE Provisions**"), foreign investment in VATS in China is limited to a maximum shareholding of 50%. This means that foreign investors looking to provide VATS in China can only access the market through a joint venture with a domestic Chinese investor.

Over the past decade, China has progressively increased the ownership thresholds for foreign investment in certain VATS under the Classified Catalogue of Telecommunications Services (the "**Telecoms Catalogue**").[73]

Preferential policies were first introduced in the Shanghai Free Trade Zone in January 2014 to ease the

72 Original texts can be found here: https://www.miit.gov.cn/zwgk/zcwj/wjfb/tg/art/2024/art_2326271e1b424e-09b6e5924ad2948863.html

73 The Telecoms Catalogue was first released in 2000 and was last revised on 6 June 2019.

foreign shareholding restrictions on 6 VATS (i.e., application stores, store and forward services, online data processing and transaction processing services to operating e-commerce business; call centre services; domestic multi-party communications services; and Internet access services to end users).[74] In 2016, special policies based on the Mainland and Hong Kong Closer Economic Partnership Arrangement ("**CEPA**") further liberalised the same 6 VATS on a nationwide basis for investors from Hong Kong and Macau.[75]

The VATS Circular is China's latest attempt to open up China's telecommunications market to foreign investors, in furtherance of the State Council 19 March 2024 action plan to boost foreign investment in China.[76]

REMOVAL OF RESTRICTIONS ON FOREIGN INVESTMENTS

The VATS Circular establishes a scheme that removes the shareholding restrictions on foreign investment in the following VATS within the Pilot Areas (the "**Pilot Scheme**"):[77]

1. Internet data centres ("**IDC**");[78]
2. Content delivery networks ("**CDN**");[79]
3. Internet access services ("**ISP Services**");[80]
4. Online data processing and transaction processing;[81]
5. Information publishing platform and transmission service (excluding internet news service, internet publishing, internet video and audio service and internet cultural service[82]); and
6. Information protection and processing services.[83]

With the exception of ISP Services, foreign investors are allowed to provide the above VATS nationwide in China through a wholly-owned subsidiary, provided that:

1. The subsidiary is incorporated in one of the eligible Pilot Areas; and
2. The subsidiary's service facilities, whether purchased or leased, are located in the city where the subsidiary is incorporated.[84]

Notably, the VATS Circular mandates Pilot Scheme ISP Services to be provided using the approved infrastructure of China's state-owned basic telecom service providers and only to users within the Pilot Areas(as opposed to the other newly-liberalised VATS, which may be provided nationwide).[85]

OTHER REQUIREMENTS

Foreign investors that intend to participate in the Pilot Scheme must meet all of the following requirements:[86]

1. Obtain prior approval from the MIIT;
2. Comply with all applicable laws and regulations during business operations; and
3. Accept and cooperate with the supervision of the MIIT and other relevant regulators.

While the VATS Circular provides a welcome relaxation by removing the shareholding restrictions for foreign investment, foreign investors are still subject to qualification requirements under the current VAT

74 See the *Opinions on Further Opening up Value-added Telecommunication Business to Foreign Investments in the China (Shanghai) Pilot Free Trade Zone*, released by MIIT in January 2014.

75 See *Circular on Related Issues of Hong Kong and Macao's Service Suppliers in Developing Telecommunications Business in the Mainland*, released by MIIT on 30 June 2016

76 Original texts can be found here: https://www.gov.cn/zhengce/content/202403/content_6940154.htm

77 Article 2, the VATS Circular

78 Categorized as B11 under the Telecoms Catalogue

79 Categorized as B12 under the Telecoms Catalogue

80 Categorized as B14 under the Telecoms Catalogue

81 Categorized as B21 under the Telecoms Catalogue

82 Categorized as B25 under the Telecoms Catalogue

83 Ibid

84 Article 2(2), the Annex of the VATS Circular

85 Ibid

86 Article 3, the VATS Circular

licensing regime, which require them to demonstrate they have:

a. a minimum registered capital of RMB 1 million (~USD 138,000) for VATS companies with business operations within a province, or RMB 10 million (~USD 1.38 million) for VATS companies with business operations beyond a single province;
b. "appropriate capital and staff" for business operations; and
c. the "*credibility and capacity to provide long-term service*".[87]

The MIIT is expected to release further details on other requirements for an approval under the Pilot Scheme and the specific documents that foreign investors will be expected to provide.

The removal of the foreign investment cap imposed on the specific VATS presents a great opportunity for non-Chinese investors in/providers of cloud, CDN, data centre and data-processing services to enter the Chinese market, or for service providers already present in the Chinese market, to increase their shareholding interests in China. With the Pilot Scheme now in place, such foreign investors and service providers may set up a wholly owned subsidiary to ensure greater control over their Chinese business operations.

Notably, while the Pilot Scheme has eased restrictions on many VATS, foreign investment in the following VATS remain subject to the 50% shareholding limit:

1. Domestic Internet Protocol - Virtual Private Network Services;[88]
2. Some Information Services (e.g., Information Search Query Service)[89]; and
3. Code and Procedure Conversion Services (e.g., Domain Name Resolution Service)[90]

Given that detailed implementation plans and rules have yet to be formulated by the local governments in the Pilot Areas,[91] many questions remain unanswered. For example, will the approval requirements differ between each of the Pilot Areas? How long will the Pilot Scheme approval be valid for? Are there any Key Performance Indicators that foreign-invested VATS providers must satisfy during the Pilot Scheme?

Of greater concern is the fact that the VATS Circular also establishes an "exit mechanism" which allows the MIIT, in its discretion, to terminate or suspend the Pilot Scheme in any Pilot Areas in any event of "frequent violations of law", "increased risks" and "lack of security supervision".[92] While the MIIT's reservation of its rights is understandable, given the perceived unpredictability of Chinese government policy, foreign VATS investors/service providers may still be cautious about entering the Chinese market, especially given the MIIT's sweeping discretion.

TAKEAWAYS

The VATS Circular is anticipated to further liberalise the Chinese telecommunications industry. Non-Chinese businesses interested in entering the China's VATS market should pay close attention to the implementation of the Pilot Scheme and keep an eye out for further clarifications on the approval requirements.

Prospective VATS entrants should also consider their strategies and structures based on the categorisation of their China businesses under the Telecoms Catalogue. While the Pilot Scheme will provide further market entry opportunities, market entrants should also be mindful of any potential risks associated with uncertainties in regulatory positions, and data compliance requirements.

THE AUTHORS WOULD LIKE TO THANK ROSLIE LIU, INTELLECTUAL PROPERTY OFFICER AT MAYER BROWN, FOR HER ASSISTANCE WITH THIS LEGAL UPDATE.

87 Articles 5 and 7, FITE Provisions; Article 13, Telecommunication Regulation of the People's Republic of China
88 Categorized as B13 under the Telecoms Catalogue
89 Categorized as B25 under the Telecoms Catalogue
90 Categorized as B26 under the Telecoms Catalogue
91 Article 1, the VATS Circular; Article 3(2), the Annex of the VATS Circular
92 Article 4, the Annex of the VATS Circular

TALK TO US

PARTNER
GABRIELA KENNEDY
HONG KONG +852 2843 2380
GABRIELA.KENNEDY@MAYERBROWN.COM

PARTNER
AMITA HAYLOCK
SINGAPORE +65 6922 2311
HONG KONG +852 6277 8579
AMITA.HAYLOCK@MAYERBROWN.COM

ASSOCIATE
JENNIFER HUANG
NEW YORK +1 212 506 2333
JHUANG@MAYERBROWN.COM

ASSOCIATE
MALEEHA KHAN
NEW YORK +1 212 506 2313
MKHAN@MAYERBROWN.COM

REGISTERED FOREIGN LAWYER (SINGAPORE)
JOSHUA WOO
HONG KONG +852 2843 4431
JOSHUA.WOO@MAYERBROWN.COM

ASSOCIATE
GRACE WONG
HONG KONG +852 2843 2378
GRACE.WONG@MAYERBROWN.COM

ABOUT MAYER BROWN

Mayer Brown is a leading international law firm positioned to represent the world's major corporations, funds, and financial institutions in their most important and complex transactions and disputes.

AMERICAS

BRASÍLIA (T&C)
CHARLOTTE
CHICAGO
HOUSTON
LOS ANGELES
MEXICO CITY
NEW YORK
PALO ALTO
RIO DE JANEIRO (T&C)
SALT LAKE CITY
SAN FRANCISCO
SÃO PAULO (T&C)
VITÓRIA (T&C)
WASHINGTON DC

ASIA

BEIJING
HANOI
HO CHI MINH CITY
HONG KONG
SHANGHAI
SINGAPORE
TOKYO

EMEA

BRUSSELS
DUBAI
DÜSSELDORF
FRANKFURT
LONDON
PARIS

Please visit mayerbrown.com for comprehensive contact information for all our offices.

MAYER|BROWN

mayerbrown.com

Americas | Asia | EMEA